Novel algorithms for protective digital privacy

Y. N. Prajapati, M. K. Srivastava
SRM University, NCR Campus, Modi Nagar, India

Article Info

Article history:

Received Apr 25, 2019
Revised Jun 26, 2019
Accepted Jul 10, 2019

Keywords:

Authentication
Compression
Cryptography
Encryption
Security

ABSTRACT

Video is the recording, reproducing, or broadcasting of moving visual images. Visual multimedia source that combines a sequence of images to form a moving picture. The video transmits a signal to a screen and processes the order in which the screen captures should be shown. Videos usually have audio components that correspond with the pictures being shown on the screen. Video compression technologies are about reducing and removing redundant video data so that a digital video file can be effectively sent over a network and stored on computer disks. With efficient compression techniques, a significant reduction in file size can be achieved with little or no adverse effect on the visual quality. The video quality, however, can be affected if the file size is further lowered by raising the compression level for a given compression technique. Security is about the protection of assets. Security, in information technology (IT), is the defense of digital information and IT assets against internal and external, malicious and accidental threats. This defense includes detection, prevention and response to threats through the use of security policies, software tools and IT services. Security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites. Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as clear text into cipher text (a process called encryption), then back again (known as decryption). Cryptography is evergreen and developments. Cryptography protects users by providing functionality for the encryption of data and authentication of other users. Compression is the process of reducing the number of bits or bytes needed to represent a given set of data. It allows saving more data. The project aims to implement security algorithm for data security. The data will be first encrypted using security techniques and that are done at the same time then it takes less processing time and more speed compression techniques will applied. If encryption and compression are done at the same time then it takes less processing time and more speed.

Corresponding Author:

Y. N. Prajapati,
SRM University,
NCR Campus, Modi Nagar, India.
Email: yogendranarayan.p@ncr.srmuniv.ac.in

1. INTRODUCTION

Need of security is to ensuring that your information remains confidential and only access to authorized user and ensure that no one has been able to change your information, so it provide full accuracy. To secure the data, compression is used because it use less disk space (saves money), more data can be transfer via internet .It increases speed of data transfer from disk to memory. Security goals are Confidential, Authentication, Integrity, and Non-repudiation [1]. Security delivers data protection across enterprise.

Data compression is known for reducing storage and communication costs. It involves transforming data of a given format, called source message to data of a smaller sized format called code word. Data encryption is known for protecting information from eavesdropping. It transforms data of a given format, called plaintext, to another format; called cipher Security goals for data security are text, using an encryption key [1]. The major problem existing with the current compression and encryption methods is the speed, the processing time required by a computer, more cost [2]. To overcome this disadvantage, combine the processes into one.

2. PROBLEM DEFINITION

For illustration of this fact, consider the Figure 1. In this shows two indifferent flows compete for bandwidth in a network containing two bottleneck links arbitrated by a fair queuing mechanism. At the first bottleneck link (R1-R2), fair queuing ensures that each flow receives 1-one-third of the link's available bandwidth (375 kbps). On the second bottleneck link (R2-S4), much of the traffic from flow B is unnecessary due to the link's limited capacity (64 kbps). Hence, flow A achieves a throughput of 375 kbps and flow B achieves a throughput of 64 kbps. Clearly, congestion collapse has occurred, because flow B packets, which are ultimately discarded on the second bottleneck link, unnecessarily limit the throughput of flow A across the first bottleneck link. Moreover, flow of A and flow of B receive equal bandwidth allocations on the first bottleneck link, their allocations are not globally max-min fair. A globally max-min fair allocation of bandwidth would have been .6572 Mbps for flow A and 64 kbps for flow B.

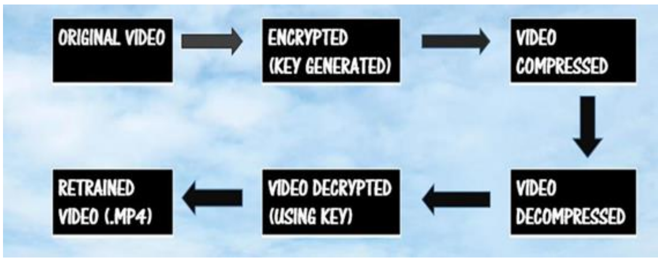


Figure 1. Block diagram

To conclude with TCP congestion control, connections may get unfairly large allocation during short round trip time as compared to larger round trip time. In recent time many have argued that such kind of issues can be resolved by use of packet scheduling mechanisms such as weighted fair queuing, core stateless fair queuing etc. But as surveyed their end results it was seen that they are able to reduce the above discussed issues but not completely eradicate them. These methods were also found expensive while implementation. In this paper we propose congestion control using the mechanism knows as Network Border Patrol. Using network border patrol we can check rate of data flow over a network. It would also help in resolving issues such as congestion collapse and unfair bandwidth allocation. It would help in preventing packet loss during transfer process, hence setting up a reliable data transfer path for source to destination.

3. EXISTING WORK

The existing secure video compression consists the encryption part separately as a software which basically make user to use two different software's which makes it a hectic task. In Existing system Compilation need to be done again for compression, Errors may occur while transmitting data, The byte/pixel relationship is unknown, Has to decompress the previous data, Slower for sophisticated methods (but simple methods can be faster for writing to disk) [3]. In existing system Video compression typically involves an elision of information not considered critical to the viewing of the video content, and an effective video compression codec (format) is one that delivers the benefits mentioned above: without a significant degradation in the visual experience of the video content, post-compression, and without requiring significant hardware overhead to achieve the compression. Even within a particular video compression codec, there are various levels of compression that can be applied (so called profiles); and the more aggressive the compression, the greater the savings in storage space and transmission bandwidth, but the lower the quality of the compressed video [as manifested in visual artefacts–blockiness, pixilated edges, blurring, rings–that appear in the video] and the greater the computing power required.

4. PROPOSED WORK

In the work a software in which we don’t need two software’s for encrypting and compression. Both the tasks can be followed one after another. Just we need to encrypt our respective file first then we can compress it send it to the destination and receiver can first decompress the file and then decrypt with the same key that the sender has set. The correct user will decrypt the file successfully. Need of security is to ensuring that your information remains confidential and only access to authorized user and ensure that no one has been able to change your information, so it provide full accuracy. To secure the data, compression is used because it use less disk space (saves money), more data can be transfer via internet. It increases speed of data transfer from disk to memory. Security goals are Confidential, Authentication, Integrity, and Non-repudiation [1]. Security delivers data protection across enterprise. Data compression is known for reducing storage and communication costs. It involves transforming data of a given format, called source message to data of a smaller sized format called code word.

Data encryption is known for protecting information from eavesdropping. It transforms data of a given format, called plaintext, to another format; called cipher Security goals for data security are text, using an encryption key [1]. The major problem existing with the current compression and encryption methods is the speed, the processing time required by a computer, more cost. To overcome this disadvantage, combine the processes into one. Video is the recording, reproducing, or broadcasting of moving visual images. Visual multimedia source that combines a sequence of images to form a moving picture. The video transmits a signal to a screen and processes the order in which the screen captures should be shown. Videos usually have audio components that correspond with the pictures being shown on the screen. Video compression technologies are about reducing and removing redundant video data so that a digital video file can be effectively sent over a network and stored on computer disks. With efficient compression techniques, a significant reduction in file size can be achieved with little or no adverse effect on the visual quality. The video quality, however, can be affected if the file size is further lowered by raising the compression level for a given compression technique. Security is about the protection of assets. Security, in information technology (IT), is the defense of digital information and IT assets against internal and external, malicious and accidental threats. This defense includes detection, prevention and response to threats through the use of security policies, software tools and IT services. Security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites.

Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit [4]. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as clear text) into cipher text (a process called encryption), then back again (known as decryption) [5]. Cryptography is evergreen and developments. Cryptography protects users by providing functionality for the encryption of data and authentication of other users. Compression is the process of reducing the number of bits or bytes needed to represent a given set of data [6]. It allows saving more data. The project aims to implement security algorithm for data security. The data will be first encrypted using security techniques and that are done at the same time then it takes less processing time and more speed compression techniques will applied. If encryption and compression are done at the same time then it takes less processing time and more speed.

5. ALGORITHM USED

– A permutation of all 256 possible bytes (denoted "S" below).

– Two 8-bit index-pointers (denoted "i" and "j").

```
i := 0
j1: =0
j2 :=0
while GeneratingOutput:
i := i + 1
    j1 := j1 + S1[i]

    swap values of S1[i] and S1[j1] output
    S2[S1[i] + S1[j1]]
    j2 := j2 + S2[i]

    swap values of S2[i] and S2[j2] output
    S1[S2[i] + S2[j2]]
```

6. BLOCK DIAGRAM

A block diagram is a diagram of a system in which the principal parts or functions are represented by blocks connected by lines that show the relationships of the blocks [7]. They are heavily used in engineering in hardware design, electronic design, software design, and process flow diagrams. Block diagrams are typically used for higher level, less detailed descriptions that are intended to clarify overall concepts without concern for the details of implementation. Contrast this with the schematic diagrams and layout diagrams used in electrical engineering, which show the implementation details of electrical components and physical construction. The block diagram shows the series of process in the simple form so that it is easy for the user to understand what is basically going to happen in the software.

7. IMPLEMENTATION

- To implement the project named “secure video compression” we need to open net bean open run our project named Data Compression, a tab asking for login password will appear. Login page as shown in Figure 2.
- Entering the login and password if existing or create a new account once you do that a other tab opens asking you for your next action which is as shown in Figure 3.
- Secure your video clicking on secure option, as soon as you click on the secure button a new tab is open to you asking you to browse the file you wish to encrypt. Encryption as shown in Figure 4.
- Once you browse the file a new tab opens asking you for a key which should be more that 8 character. Encryption key as shown in Figure 5.
- After entering the key the software will ask you the destination you want to save file select a place to find comfortable to reach and you don’t forget before further for compression you need the same encrypted file.
- Now open the compress data part of the tab opened after you logged in as shown in Figure 6.
- Once you select the compress data part you will be asked to browse the file you want to compress be sure you select the encrypted file and it also ask you for destination you want to add compressed file too as shown in Figure 7.

Select the video you want to compress and select the compress button you will be able to see the compression ratio of original file to compressed file in the status bar after the compression is done save the file to a destination of your choice and send it to the receiver through your network. Once the receiver receive the file he or she will decompress and decrypt the file using the same key sender encrypted the file with.

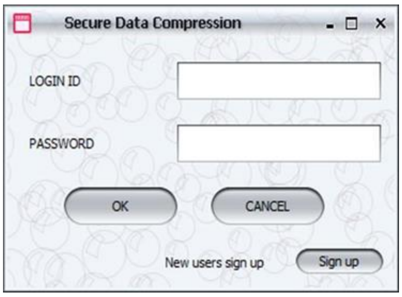


Figure 2. Login page

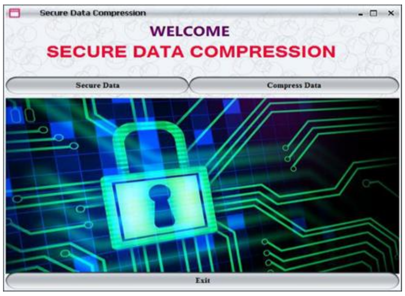


Figure 3. Welcome page

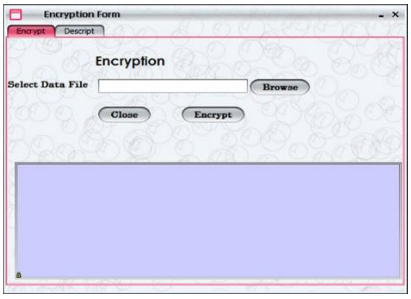


Figure 4. Encryption

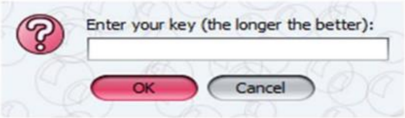
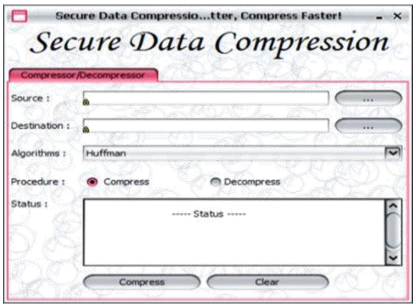


Figure 5. Encryption key



Algorithms : Huffman

Procedure : ● Compress ○ Decompress

Figure 6. Compress button

Figure 7. Compression blog

8. CONCLUSION

In this paper we evaluate the performance with respect to different parameters. It shows basic information about cryptography and compression, & their techniques are applied on file. For security, combination of compression and cryptographic technique is used. To secure our data more that's why we encrypt the data first and then compressed data. It has many advantage of doing this we can transfer more and more data via internet. If combination is used it may be less costly, it save time, more secure.

9. FUTURE WORK

The secure video compression project have lot of future scope as today people are dependent on networks for their files transfer and information gathering. This project helps a person to encrypt the data before compressing it and after compression when the file is sent to the destination receiver has a key given by the sender with the help of which the receiver can decompress the file first then decrypt it. Key management is a critical issue in all encryption based security systems, as it cannot be separated from the design of secure multimedia distribution. In most distribution architectures, multimedia content is encrypted with asymmetric key which also needs to be protected in transmission to the receiver. Hence, the storage and security requirements of key management need to be discussed in greater detail in future proposals. Another feature that may be added to the proposed selective schemes is the selection criteria. Encryption techniques can be chosen dynamically as the content is being distributed and the selection criteria can be changed as needed by the application. Enhancement in compression performance by introduction of new functionalities which also improves security as encryption is combined with compression.

REFERENCES

[1] Mr. Vinod Saroha, Suman Mor, Anurag Dagar "Enhancing Security of Caesar Cipher by Double Columnar Transposition Method," *International Journal of Advanced Research in Computer Science and Software Engineering*, ISSN: 2277 128X, Volume 2, Issue 10, 2012.

[2] Senthil Shanmugasundaram, Robert Lourdusamy "A Comparative Study Of Text Compression Algorithms," *International Journal of Wisdom Based Computing,* Vol.1 (3), December 2011.

[3] Harshraj N. Shinde, Aniruddha S. Raut, Shubham. Vidhale, Rohit V. Sawant, Vijay A. Kotkar, "A Review of Various Encryption Techniques," *International Journal of Engineering And Computer Science* ISSN: 2319-7242, Volume 3, Issue 9, September 2014.

[4] Ms. Ayushi Aggarwal, Anju "Enciphering Data for Larger Files," *International Journal of Advanced Research in Computer Science and Software Engineering*, ISSN: 2277 128X, Volume 3, Issue 5, May 2013.

[5] Sombir Singh, Sunil K. Maakar, Dr. Sudesh Kumar "Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques," *International Journal of Advanced Research in Computer Science and Software Engineering*, ISSN 2249-6343, Volume 2, Issue 1, Jan 1965.

[6] A L. Jeeva, Dr. V. Palanisamy, K. Kanagaram "Comparative Analysis of Performance Efficiency and Security Measures of Some Encryption Algorithms," *International Journal of Engineering Research and Applications (IJERA)*, ISSN: 2277 128X, Volume 3, Issue 6, June 2013.

[7] T. Subhamastan Rao, M. Soujanya, T. Hemalatha, T. Revathi, "Simultaneous data compression and encryption," *(IJCSIT) International Journal of Computer Science and Information Technologies*, ISSN 0975-9646, Volume-2(5), 2011.