Available Online at http://www.recentscientific.com

ISSN: 0976-3031

International Journal of Recent Scientific Research
Vol. 6, Issue, 7, pp.5521-5524, July, 2015

International Journal of Recent Scientific Research

RESEARCH ARTICLE

PRIVACY PROTECTION FOR VIDEO, IMAGE, TEXT TRANSMISSION

Shraddha Bhatte[1], J. W. Bakal[2] and Madhuri Gedam[3]

[1,3]Department of Computer Engineering, Shree L. R. Tiwari College of Engineering, Mumbai University, Thane, Maharashtra, 401107, India

[2]Principal, Shivajirao S. Jondhale College of Engineering, Mumbai University, Thane, Maharashtra,421204, India

ARTICLE INFO

Article History:

Received 14th, June, 2015
Received in revised form 23th, June, 2015
Accepted 13th, July, 2015
Published online 28th, July, 2015

Key words:

H.264/AVC , Compression ,Scrambling ,Encryption ,privacy protection.

ABSTRACT

From last few years electronic data is become part of daily life ,this data is used from educational purpose to financial purpose ,from common man to big business houses .this e- data contain video, image ,and text.as the use of e-data increases ,the problem of security to this data is also increase . To provide the protection to e-data it is essential to have robust privacy protection system .proposed paper is going to focus on solid privacy protection system by using existing algorithm in the market .and also try to provide efficient data transfer.

INTRODUCTION

Recently Techniques for hiding electronic information have got very importance in a number of application areas. Digital video, image and text are increasingly furnished with different but imperceptible marks, which may contain very crucial data like a hidden copyright notice or serial number or even help to prevent unauthorised copying directly. Military communications systems make increasing use of electronic data transfer for communication, this information contain very high confidential data which, rather than merely concealing the content of a message using encryption, seek to conceal its sender, its receiver or its very existence. Similar technologies are used in various electronic system which is used for communication.[1]

As the new technics for electronic data hiding are increasing, the people who are interested in breaking that security, means e- Criminals are also increasing. In such scenario making electronic data transfer safe by increasing data protection system robust is very necessary.

The proposed article focus on providing security ,by using layers of data hiding technics ,the proposed system mainly focus on three types of electronic data like Video, Image and text.

Problem definition

To ensure the security of electronic data while transferring through networks, different security techniques are used. Like every process, encryption and decryption processes involve use of CPU recourses like CPU cycle memory. These processes require good amount of time for I/O, encryption and decryption operation. Hence these security algorithms consume a good amount of resources for encrypting and decrypting the data. So it is essential for an encryption algorithm to have good performance along with the security.[5,6,7]

To prevent data loss during transmission and to promote faster transmission, many different compression algorithms are used to reduce the size of the data during transmission. Usually lossless compression algorithms are used if data that is being transferred is important and if data loss is not affordable.

If a compressed file is encrypted, it has better security and faster transfer rate across the network than encrypting and transferring uncompressed file. But in some cases, compression increases the overhead like size of file and processing time etc. Hence there is a need to analyse different compression and encryption algorithms for various parameters so as to understand the factors that can affect the performance of this algorithms. Also identify whether the file that has to be

Corresponding author:* **Shraddha Bhatte
Department of Computer Engineering, Shree L. R. Tiwari College of Engineering, Mumbai University, Thane, Maharashtra, 401107, India

compressed before encrypting or not. If compression is needed then identify the best suitable compression algorithm that should be used for compressing the file according to data type and data size to reduce the overhead of time for compression and increase the efficiency and security to data that is being transferred

For achieving faster communication most of confidential data is circulated through networks as electronic data. Many different computer applications in different domains exchange a lot of confidential data. [2,3]

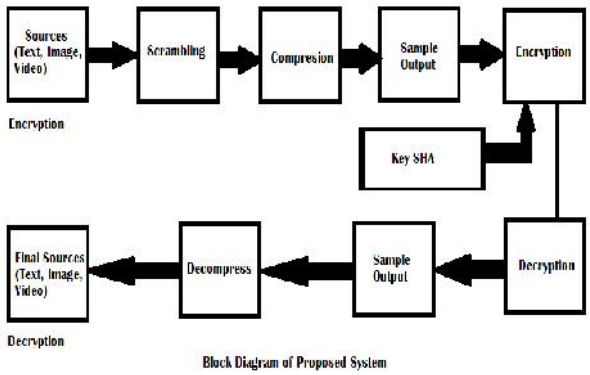
The field of health care and electronic health care records is one such example. Some of the computer applications related to field of health care are not secure. Health related data has different data formats like image, textual and video data formats etc. Most of this data is confidential and needs to be transmitted securely.

Compression, Scrambling and Encryption play an important role in securing this confidential data against unauthorized attacks. Therefore, along with security, factors like implementation cost and performance of different Compression, Scrambling and Encryption algorithms also need to be considered for practical implementation.

Parameters like data type, data size, compression ratio, key size, key strength, encryption time, decryption time affects the selection of algorithm and therefore we need some benchmark for selection of security algorithm. If the file size is small, encryption and transfer of such files can improve the performance of the system to some extent. For this, a file may be first scramble then compressed and then encrypted. Using this three technic we can achieve robust security and better performance also.

Proposed system

Following diagram shows the proposed system for privacy protection for video, image and text transfer.



Block Diagram of Proposed System

Proposed system used combination of very simple and existing algorithm to provide privacy protection to data which is to be transferred.

In proposed system H.264/AVC algorithm is use for scrambling and compression of video, image. Encryption is done using SHA-1 and AES/DES algorithms

Hardware and software details used for impelementation of proposed system:

1. JAVA 1.7
2. Two Personal computers
3. Networking Devices (Network cable/HUB/Router i.e. depends on the network topology)
4. Any operating system (Linux/windows)

Advantages of hardware and software

- As we are using java as programming language, ultimately we are getting platform independence facility.
- H.264 provides higher level security.
- No need to use separate system for image / Text / Video, same proposed system can be used for video, image and text
- Bandwidth require lesser than existing system.
- Cost reduces as we are using single system for three type of electronic data.
- Speed increases

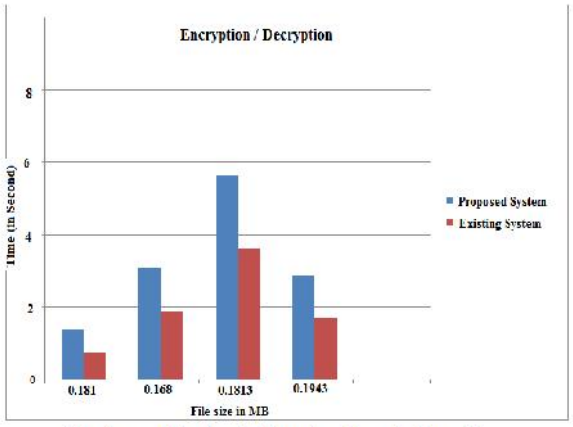
RESULT ANALYSIS

In this section I would like to discuss result of proposed system. We have compared total five sample of video, image and text file. Result of it as follows.

Following table gives the real testing values of five sample of video, image, text, which is tested using proposed system. The sample are tested on the basis of transfer duration, packet transfer ,original file size and the compress file size and speed of total data transfer. This results are compare with existing system which clearly gives the difference with existing system compare to existing system speed of file transfer increased, compression ratio is high, and security level also very high.

Table 1 result of image testing

Image file	Origanal size	Transfer duration	Packets transfer	File size	Speed
IMG1.JPEG	1.72 MB	0.1069 SEC	24	0.1811 MB	1.69 MB/SEC
IMG2.JPEG	1.99MB	0.0678 SEC	22	0.1681 MB	2.47 MB/SEC
IMG3.JPEG	1.65MB	0.0314 SEC	24	0.1813MB	5.77 MB/SEC
IMG4.JPEG	1.80MB	0.0912 SEC	26	0.1943 MB	2.13 MB/SEC



Time (in seconds) requires for Encryption / Decryption Image file

Fig.2 comparisons of testing result of image file, proposed system with existing system

Table 2 Result of video testing

viedo file	transfer duration	packets transfer	origanal file size	compress file size	speed
20131228_004340.mp4	27 SEC	1576	178.685MB	12.1837 MB	45.12 MB/ SEC
TEXT2.MP4	12.33 SEC	856	38.5 MB	6.6152 MB	53.65 MB/ SEC
TEXT3.MP4	0.9 SEC	655	12.07 MB	5.06 MB	53.774 MB/ SEC
TEXT2.MP4	13 SEC	966	31.191MB	7.74 MB	57.025 MB/ SEC

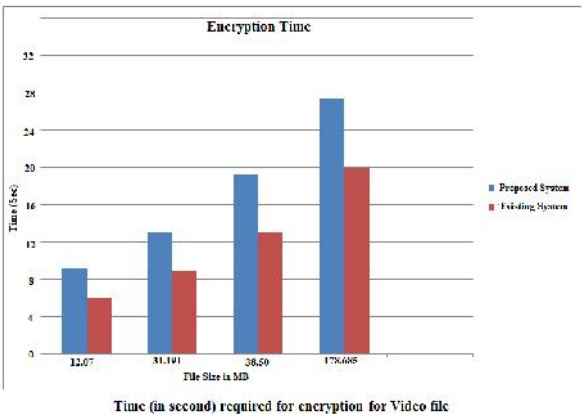


Fig 3 comparisons between proposed systems with existing system according to encryption time

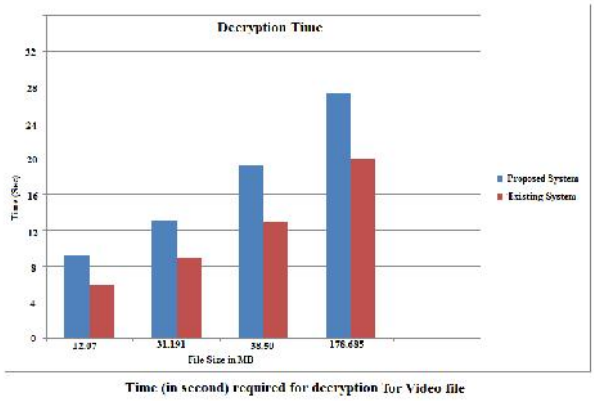


Fig.4 comparisons between proposed systems with existing system according to decryption time

Table 3 Result of Text document testing

Text file	Origanal size	Transfer duration	Packets transfer	File size	Speed
TEST1.TXT	15KB	0.0085 SEC	2	0.0139 MB	1.639 MB/SEC
TEST2.TXT	55KB	0.0161 SEC	7	0.0531 MB	3.29 MB/SEC
TEST3.TXT	12KB	0.0124 SEC	2	0.0112 MB	0.9069 MB/SEC
TEST4.TXT	272KB	0.12 SEC	35	0.2653 MB	2.0423 MB/SEC

If we compare the existing system result with our proposed system we get following comparison results

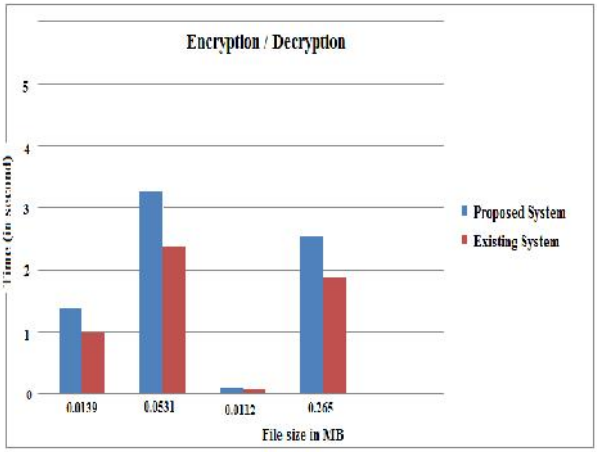


Fig.5 comparisons between proposed systems with existing system according to decryption time

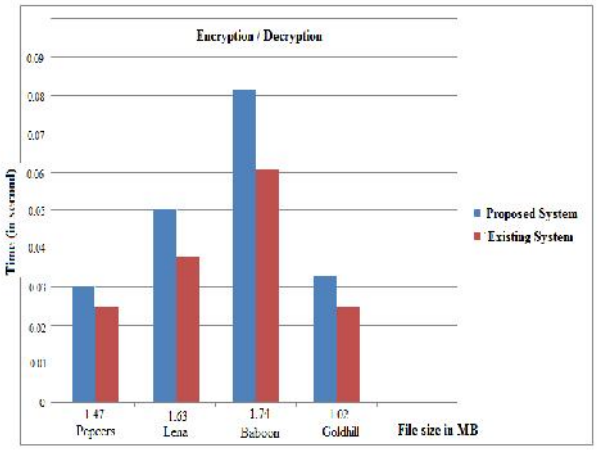


Fig.6 comparisons between proposed systems with existing system according to encryption/decryption time

Table 4 comparison of existing system with proposed system

Image file	Transfer duration	Packets transfer	Original file size	Exexting cr	Propsed cr	Speed
Pepeers.JPEG	0.039 SEC	2	40.3 KB	1.47527MB	0.0103MB	2.64 MB/SEC
Lena.JPEG	0.005 SEC	2	38.3 KB	1.74454MB	0.01 MB	19.928 MB/SEC
Baboon.JPEG	0.008 SEC	3	78.1 KB	1.63038MB	0.0196MB	24.52 MB/SEC
Goldhill.JPEG	0.003 SEC	2	48.6 KB	1.0274 MB	0.016 MB	35.1969 MB/SEC

Table 6 comparison between existing system and proposed system

Text name	Compression		Speed		Security	
	Existing System	Proposed System	Existing System	Proposed System	Existing System	Proposed System
Text	50% approx	Less than 50%	Low	High	Low	High
Image	50% approx	Less than 50%	Low	High	Low	High
Video	50% approx	Less than 50%	Low	High	Low	High

CONCLUSION

If Work has been done on some limitation of proposed syem there is wide area of application where we can use our system. If results given in table is considered then the output of proposed system can be use in existing messenger as a attachment to send big size of data securely. The standard provides integrated support for transmission or storage, including a pocketsize compressed format and features that help to minimize the effect of transmission errors.

References

1. F. Dufaux and T. Ebrahimi, "Recent Advances in MPEG-7 Cameras", in SPIE Proc. Applications of Digital Image Processing XXIX, San Diego, CA, August 2006
2. F. Dufaux and T. Ebrahimi, "Scrambling for Video Surveillance with Privacy", in IEEE Proc. Workshop on Privacy Research In Vision, New York, NY, June 2006.
3. F. Dufaux, and T. Ebrahimi, "Video Surveillance using JPEG 2000", in SPIE Proc. Applications of Digital Image Processing XXVII, Denver, CO, Aug. 2004
4. T.E. Boult, "PICO: Privacy through Invertible Cryptographic Obscuration", IEEE/NFS Workshop on Computer Vision for Interactive and Intelligent Environments, Nov. 2005
5. W. K. Cham, Family of order-4 four level orthogonal transforms, Electron. Lett. 19 (21) (October 1983)
6. W.K. Cham, R.J. Clarke, Simple high efficiency transform for image coding, in: Proceedings of the International Picture Coding Symposium, Davis, CA, 1983, pp.66–67
7. Z. Shahid, R. Eifrig, A. Luthra, K. Panusopone, Coding of an arbitrary shaped interlaced video in MPEG-4, in: Proceedings of the IEEE International Conference on Accoustics, Speech and Signal Processing (ICASSP'99), 2009 pp. 3121–3124

How to cite this article:
Shraddha Bhatte *et al*., Privacy Protection For Video, Image, Text Transmission. *International Journal of Recent Scientific Vol. 6, Issue, 7, pp.5521-5524, July, 2015*

****