ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Privacy Protection for Video, Image, Text Transmission

Shraddha Bhatte, Dr. J. W. Bakal, Madhuri Gedam

Student, Department of Computer Engineering, Shree L. R. Tiwari College of Engineering, Mumbai University, Thane, Maharashtra, India

Principal, Shivajirao S. Jondhale College of Engineering, Mumbai University, Thane, Maharashtra, India

Assistant Professor, Department of Computer Engineering, Shree L. R. Tiwari College of Engineering, Mumbai University, Thane, Maharashtra, India

ABSTRACT: In this paper, we are going to discuss the problem of privacy protection in electronic data transfer systems . Electronic data is consist of video, image , and text . Providing protection is not sufficient for effective data transfer .it is also important to regulate all parameters of data transfer. like speed , bandwidth required ,size ,PSNR ratio .etc. ,we basically achieving both the things by using H.264/AVC algorithm ,and 256 bit encryption key. Because of it we get three layers of protection as well as efficient data transfer rate.

KEYWORDS:H.264/AVC algorithm, scrambling, compression, encryption.

I. INTRODUCTION

With the widespread use of media transfer systems, The issue of electronic data privacy is increasingly becoming prominent. While transmitting data like video, image or text there is always fear of insecurity due to terrorist threats and high criminality rate, Because of this the rightful fear of privacy invasion is converting into a significant concern. From last few years, multimedia data such as video, text, and image are used in more and more applications, such as video conference, video-on-demand ,airports ,banks ,e-learning etc. The data used in all this technique should be transfer securely from sender to receiver but with the rapid development of multimedia processing technologies, digital video, text or images can be easily changed, tampered, altered or forged by unauthorized users . Which can cause big loss which can not be bearable in business.

Just providing security to network is not sufficient. There is also need of providing security to data which is transmitting on the network. There are so many ways to providing security to multimedia data like providing password , water marking , encryption etc. as multimedia data is very huge it required very large processing. While processing multimedia data we have to think about various parameters like computational efficiency ,speed ,compression ratio ,encryption ratio, security, format Compliance so on As per application of multimedia data level of security differs for example for video on demand ,medical data required low level of security where as military purpose or financial application demands for very high level of security.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

II. RELATED WORK

High level Security system proposed for multimedia data ?

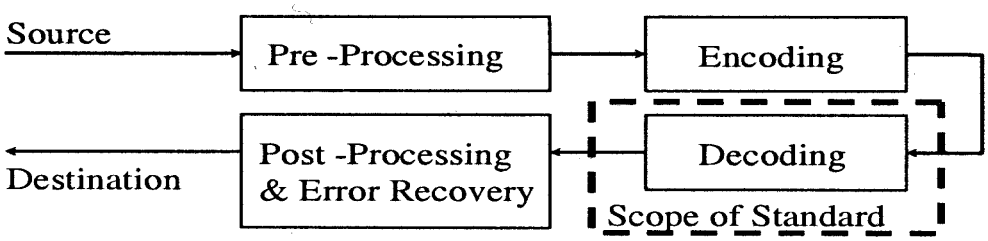


Fig 1. Above shows the area where the high level security required [5]

Information hiding techniques have recently become important in a number of application areas. It is often thought that communications may be secured by encrypting the traffic, but this has rarely been adequate in practice. [1]

This paper concentrated on methods for hiding messages rather than for enciphering them.The main aim of this paper is privacy protection of multimedia transmission .here focus is mainly on video, image and text. Security to media (video, image ,text) transmission will give in three layers .According to literature survey most of the existing systems used one layer of protection that is either scrambling or compression otherwise only encryption but as per the recent market need only one layer protection for maintain privacy of the media (video ,image ,text) transfer is not sufficient.[2,3] Also it is important to maintain all basic parameters like bandwidth, compression ratio, PSNR ratio, speed of transmission, quality of product after transmission, and total cast of transmission adequate.

III. PROPOSED DESING

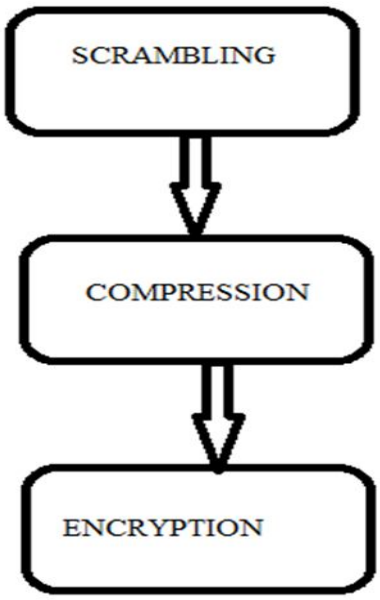


Fig 1: Diagram of proposed system

Along with privacy protection, it is important to maintain all basic parameters like bandwidth, compression ratio, PSNR ratio, speed of transmission, quality of product after transmission, and total cast of transmission adequate.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

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

Section [1]: **H.264/AVC:**

In proposed system for providing protection to multimedia data like video and image .we use H.264/AVC algorithm. The main function of H.264/AVC is to provide both compression as well as scrambling. [8]

H.264 is a block-based, motion-compensated video compression method. It is designed to be scalable, that is, its efficiency is roughly equally high for all purposes from low-bandwidth streaming up to high definition broadcast and storage.

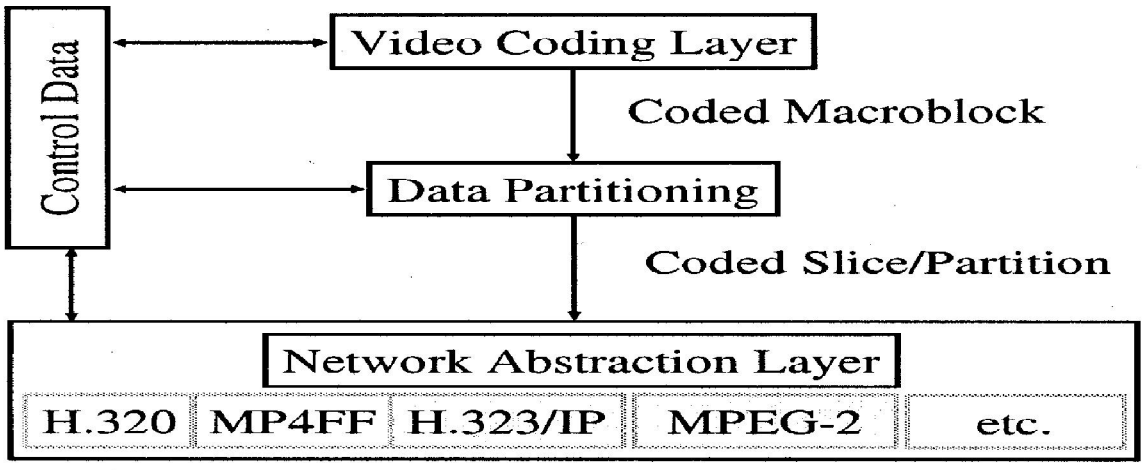
H.264 FEATURES:

H.264/AVC/MPEG-4 Part 10 contains a number of new features that allow it to compress video much more effectively than older standards and to provide more flexibility for application to a wide variety of network environments. In particular, some such key features include: [6]

- Multi-picture inter-picture prediction.
- Variable block-size motion compensation
- The ability to use multiple motion vectors per macro block.
- Quarter-pixel precision for motion compensation.
- Spatial prediction from the edges of neighbouring blocks for "intra" coding.
- Flexible interlaced-scan video coding features.
- New transformation design features.
- An entropy coding design including context adaptive binary arithmetic coding and Context adaptive variable-length coding.

H.264 APPLICATION

- The H.264 was designed to be flexible video format and has a very broad application range including [5]
- Low bit-rate Internet streaming applications.
- HDTV broadcast and Digital Cinema applications.
- Web software embedding.
- Mobile TV standardization.
- Video conferencing products.
- SDTV and HDTV standardization and deployment.
- HD Video Storage applications.



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Following fig.1 shows the basic diagram of H.264/AVC encoder [4]In proposed paper H.264/AVC provides mainly two functionality

1) Compression
2) Scrambling

Section[2] :Compression :

What is Video or image compression?

Video compression is about reducing and removing redundant video data so that a digital video file can be effectively sent and stored. The process involves applying an algorithm to the source video to create a compressed file that is ready for transmission or storage. To play the compressed file, an inverse algorithm is applied to produce a video that shows virtually the same content as the original source video. The time it takes to compress, send, decompress and display a file is called latency. The more advanced the compression algorithm, the higher the latency, given the same processing power.

A pair of algorithms that works together is called a video codec (encoder/decoder). Video codecs that implement different standards are normally not compatible with each other; that is, video content that is compressed using one standard cannot be decompressed with a different standard. [11]

Different video compression standards utilize different methods of reducing data, and hence, results differ in bit rate, quality and latency.

Data compression is a method of reducing the size of the data file so that the file should take less disk space for storage. The file that contains redundancy gets reduced by compression. Proposed paper uses following compression algorithm:

a. Lossy compression algorithms
b. Lossless data compression algorithms

Lossy compression algorithms

In lossy data compression algorithms there is loss of original data while performing compression. In computer science and Information technology, a data encoding method in which the data is compressed by losing some amount of data is lossy compression.

Lossless data compression algorithms

In case of lossless data compression algorithm there is no data loss while compressing a file, it guarantees to reproduce the exactly same data as input. If data loss is not desirable the lossless data compression algorithms should be used. Some of the 5 peculiar examples include executable text documents, programs and source codes etc. Some of the image file formats also uses lossless compression[9]

Section[3]:Scrambling:

A scrambling approach is a method which is employed on almost all commercially manufactured system including image and video systems. The basic purpose of scrambling is content protection

A valuable content scrambling approach is a raising issue as protecting contents copyright is important. Image and video scrambling is well employed, and its general way is to hide unwanted information and disclose UN interpretable image and video. There have been many methods regarding image and video scrambling [14]

In proposed paper for video scrambling block shuffling is used and for image ROI scrambling is used.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

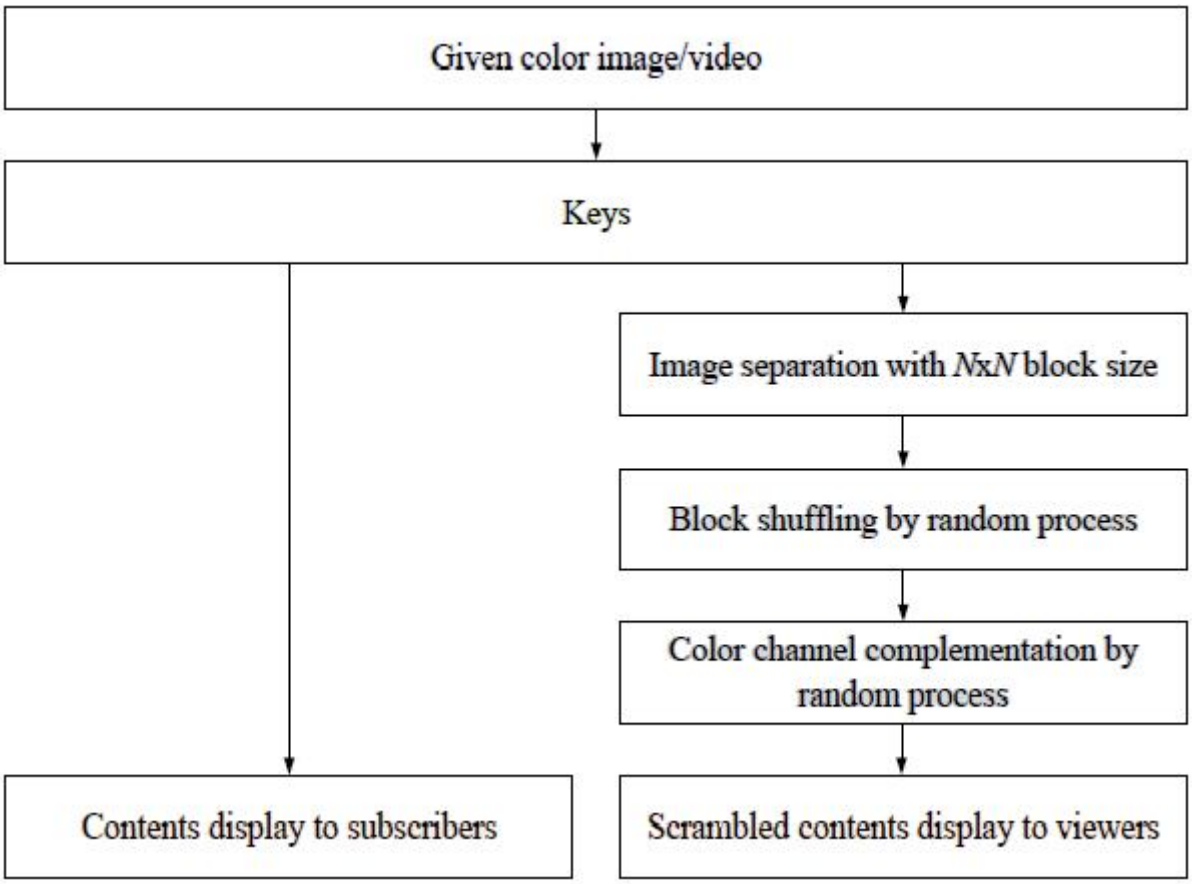


Fig2: Block diagram for scrambling by block shuffling

Random sign inversion:

The scrambling process should not have a negative impact on coding efficiency. A natural choice is therefore to apply scrambling to the AC coefficients. Furthermore, whereas the amplitude of AC coefficients is correlated, their signs are not as.per consequent, we propose to scramble the quantized AC,Straight forwardly, this technique requires negligible computational complexity. Random sign inversion can be expressed as follows**.**

$$qACcoeff[i] = \begin{cases} -qACcoeff[i] & if\ random\_bit = 1 \\ +qACcoeff[i] & otherwise \end{cases}$$

Random permutation:

Alternatively, we propose a second scrambling method applying a random permutation to rearrange the order of AC coefficients in 4x4 blocks corresponding to MB in the foreground slice. The random permutation can be expressed as

$$\begin{pmatrix} 0 & 1 & \dots & 14 & 15 \\ x_0 & x_1 & \dots & x_{14} & x_{15} \end{pmatrix}$$

Section [3] Encryption:

According to previous work only scrambling and compression doesn't provide strong security against security breach, so to provide extreme security proposed system applies 256 bit encryption key on data packet .

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Why 256 bit Key?

The Main Reason behind it is, number of combination we get .that's means we can create so many keys , for example 2^256 key's we can create ,so difficulty level for crack this password is very very high . so protection level is also high.

For generating this key we used SAH-1 and AES/DES algorithm.

IV. RESULTS AND DISCUSSION

Proposed system gives very good compression ratio then existing system .we almost compress system by 80% at the time of encryption .and at the time of decryption there is no change in image ,received image almost of same size. Proposed system give us very high level of security because of layers of protection. Compression time ,encryption time ,speed of data transfer is very high. Same proposed system can be use for sender as well as receiver side. So its very easy to handle as well as same time of system use for all type of data so .cost of data transfer is reduced .following comparison table of existing system with proposed system is self -explanatory

Table 1: Comparison between existing system and proposed system

IMAGE FILE	TRANSFR DURATION	PACKETS TRANSFER	ORIGINL FILE SIZE	EXEXTIG CR	PROPSD CR	SPEED
Pepeers.JPG	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	0.019 MB	24.52 MB/SEC
Goldhill.JPG	0.003 SEC	2	48.6 KB	1.0274 MB	0.016 MB	35.1969 MB/SEC

V. CONCLUSION AND FUTURE WORK

In this paper, we have discussed "Privacy protection for video, image, text transmission" Why it is required. We have taken over view the various algorithms and methods for information hiding, scrambling and compression and AES/DES. On basis proposed paper we can ensure a a "network-friendly" multimedia data Transmission addressing "conversational" (video telephony) and "non conversational" (storage, broadcast, or streaming) applications

REFERENCES

[1] ThomasSt¨utz and Andreas Uhl,, "A Survey of H.264 AVC/SVC Encryption', Technical Report,2013
[2]Frederic Dufaux and TouradjEbrahimi,"Scrambling for privacy protection in video surveillance systems". IEEE Transactions , 2008
[3] GwanggilJeon "Block Shuffling Approach for Contents Protection", ' International Journal of Security and Its Applications , 2014
[4] Thomas Wiegand, Gary J. Sullivan,GisleBjøntegaard, ,AjayLuthr, "Overview of the H.264/AVC Video CodingStandard",IEEETRANSACTIONS,2003
[5] "Fabien A.P. Petitcolas, Ross J. Anderson, and Markus G. Kuhn "Information hiding-a survey IEEE , 1999
[6] Qiuhua Wang, XingjunWang , "A New Selective Video Encryption Algorithm for the H.264 Standard", IEEE,2014
[7] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn . "Information Hiding|A Survey", *IEEE*,1999.
[8]D. Chaum"Untraceable electronic mail, return addresses and digital pseudonyms.",*Communications of the A.C.M.*,1981.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

[9]Frederic Dufaux and Touradj Ebrahimi,"H.264/AVC VIDEO SCRAMBLING FOR PRIVACY PROTECTION", IEEE, 2008

[10] A.W. Senior, S. Pankanti, A. Hampapur, L. Brown, Y.-L. Tian, and A Ekin,. "Blinkering Surveillance: Enabling Video Privacy through Computer Vision", IBM, 2003.

[11] F. Dufaux, and T. Ebrahimi "Video Surveillance using JPEG 2000", , SPIE ,2004.

[12]F. Dufaux and T. Ebrahimi , "Scrambling for Video Surveillance with Privacy", IEEE, 2006

[13] T.E. Boult ,"PICO: Privacy through Invertible Cryptographic Obscuration", IEEE, Nov. 2