iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** IV **Month of publication:** April 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Different Reviews on Video Encryption Using Transform and Coding

Manisha Sharma[1] Kamaljeet Kaur[2]
[1,2]Electronics and communication, JMIT Radaur

Abstract— Multimedia networks such as multimedia electronic mail, Internet television, and video conferences are included among communication systems with high transmission rate in computer and communication networks. Multimedia encryption challenges originate from two realities: firstly, multimedia data have great volumes. Secondly, they need real-time uses. So, using encryption for security results in additional computations for information processing. As a result, a balance between security and synchronization requirement is necessary. To reach this aim, we use lightweight and high-speed encryption algorithms need to encrypt the video sequence of frames. In the current work we are going to present the different reviews of Video encryption.

Keywords— Multimedia, Compression, advanced encryption standard (AES), Discrete cosine transform (DCT), Discrete wavelet transform (DWT).

I. INTRODUCTION

The science of encryption and decryption of messages so as to keep these messages secure is called cryptography. In cryptography, encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption doesn't prevent hacking but it reduces the likelihood that the hacker will be able to read the data that is encrypted. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable cipher text. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the cipher text should not be able to determine anything about the original message. An authorized party, however, is able to decode the cipher text using a decryption algorithm which usually requires a secret decryption key that adversaries do not have access to it .For technical reasons, an encryption scheme usually needs a key-generation algorithm to randomly produce keys.

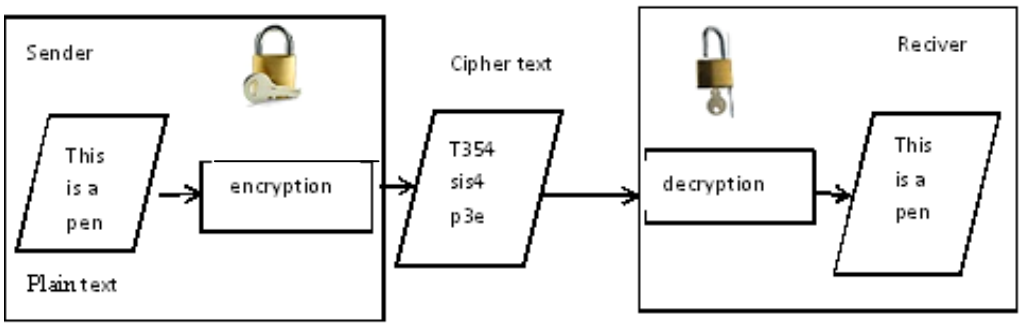


Fig. 1 Block Diagram of cryptography.

A. Encryption

Encryption has long been used by militaries and governments to facilitate secret communication. It is now commonly used in protecting information within many kinds of civilian systems. For example, the Computer Security Institute reported that in 2007, 71% of companies surveyed utilized encryption for some of their data in transit, and 53% utilized encryption for some of their data in storage. Encryption can be used to protect data "at rest", such as files on computers and storage devices (e.g. USB flash drives). In recent years there have been numerous reports of confidential data such as customers' personal records being exposed through loss or theft of laptops or backup drives. Encrypting such files at rest helps protect them should physical security measures fail. Encryption is also used to protect data in transit, for example data being transferred via networks (e.g. the Internet, e-commerce), mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices and bank automatic teller machines. There have been numerous reports of data in transit being intercepted in recent years. Encrypting data in transit also helps to secure it as it is often difficult to physically secure all access to networks. Decryption is the process of converting data from encrypted format back to their original format. Data encryption becomes an important issue when

sensitive data are to be sent through a network where unauthorized users may attack the network. These attacks include IP spoofing in which intruders create packets with false IP addresses and exploit applications that use authentication based on IP and packet sniffing in which hackers read transmitted information. One of the applications that are attacked by the hackers is the E-mail. There are many companies providing the E-mail service such as Gmail, Hotmail and Yahoo mail. These companies need to provide the user with a certain data capacity, speed access, as well as a certain level of security. Security is an important issue that we should consider when we choose Web Mail. Some of the techniques that are used to verify the user identity (i.e. to verify that a user sending a message is the one who he claims to be) are the digital signature and the digital certificate. There are some standard methods which are used with cryptography such as private-key (also known as symmetric, conventional, or secret key), public-key (also known as asymmetric). In private-key cryptography, a single key is used for both encryption and decryption. This requires that each individual must possess a copy of the key and the key must be passed over a secure channel to the other individual. Private-key algorithms are very fast and easily implemented in hardware. Therefore they are commonly used for bulk data encryption. Image encryption schemes have been increasingly studied to meet the demand for real-time secure image transmission over the Internet and through wireless networks. Traditional image encryption algorithm such as data encryption standard (DES), has the weakness of low-level efficiency when the image is large.

B. Needs Of Cryptography

With the development of computer technology and internet technology, the requirement of video data is used more and more in Human's life. In order to protect multimedia data about polities, Economic and military, some multimedia encryption algorithm has been proposed. Video data can be encrypting in two ways: One way to ensure content privacy is to encrypt video data as a whole is called "fully confidential" video encryption algorithms. These applications include video conferencing and video telephony, as well as video transmission for financial or military purposes. Even though this approach provides security, implementation is costly due to huge size of video data. Other way is to encrypt the video data by selective video content this type of security is suitable for video signals which have a huge volume and need to be processed in real time .This is called perceptually video encryption and these used in various applications such as video transmission for entrainment, such as video-on-demand (VoD), pay -TV and live video broadcasting. The encryption criteria are in two ways: (1) Persons are likely to become subscriber if they get interest from down-graded video sequence.(2) the video signal is encrypted to a certain extent so that only customers who have paid for the service can obtain the high-quality version. This algorithm must not add extra overhead to increase the size of video data which is already huge. Furthermore, security must also obey to the real time operation constraints at decoder side, which means that they must be quick and simple enough not to disturb the decoding process. As usual, they must also provide a good level of content privacy.

II. RELATED WORK

Bing Zeng,, Siu-Kei Au Yeung (2014): In this paper, The authors has described for transform domain for perceptual encryption of video signals in which multiple transforms are designed by using different rotation angles at the final stage of the discrete cosine transforms (DCTs) butterfly flow-graph structure. More recently, it is found that a set of more efficient alternative transforms can be derived by introducing sign-flips at the same stage, which is equivalent to an extra rotation angle of π and also they put their research to generalize this sign-flipping technique by randomly embedding sign-flips into all stages of the DCTs butterfly structure so that the encryption space becomes much larger to yield a higher security.[1,2,3]

Oi-Yan Lui, Kwok-Wo Wong (2013): In this paper, A chaos based selective encryption schemed has been proposed on the H.264/AVC standard. To mask the selected H.264/AVC syntax elements four digitized Renyi chaostic maps employed to generate a pseudorandom bit sequence. The proposed algorithm is highly sensitive to the secret key and possesses good perceptual security. the proposed algorithm offers a format compliant, fast and secure selective encryption of H.264/AVC video sequences by destroying their commercial values.[4]

Shiguo Lian , Xi Chen (2013):Partial encryption is also known as selective encryption. It has the properties of time efficiency, format compliance and network compliance; hence it is a suitable choice for multimedia content encryption. They presented a partial encryption model with some secure encryption principles with respect to the existing attacks(cryptographic attack, replacement attack and statistical model based attack. they also proposed a partial encryption scheme in wavelet domain which proved the principles appropriate for designing of multimedia encryption schemes along with its performance .[5]

Saeed Bahrami, Majid Naderi (2013): In this paper, A Lightweight stream cipher and fast algorithms having time efficiency, high execution speed, usually used in frequency transform domain and in a partial encryption form, were proposed to encrypt multimedia content with compression structures. In this article, two designs were introduced for select DCT transform coefficients by the stream encryption algorithm based on three fundamental principles and confronting the partial encryption attacks such as cryptographic attack, replacement attack and statistical model based attack. The speed of the proposed algorithm

is faster as compared to A5/1 and W7 stream ciphers. The results show that the proposed encryption algorithm in two designed for partial encryption of DCT transform coefficients are applicable for real-time multimedia security applications requiring fast computation and earn sufficient security levels.[8]

Gul Boztok Algin, E. Turhan Tunali (2011):The authors proposed a new algorithm H.264 SVC (Scalable Video Codec) together with constraints arising from structural properties of the SVC software for encryption. The result from the new algorithm has find that no overhead with low level encryption and acceptable overhead for high level encryption that leads to totally unperceivable video. In this paper, authors also observed that the visual degradation for different type of videos independent from the motion and resolution characteristics is almost same. [7]

Xiaofeng Wang, Nanning Zheng , Lihua Tian (2010): The authors proposed an improved comprehensive video encryption scheme, in which, the intra-prediction mode, motion vector difference, and quantization coefficients encrypted efficiently. the encryption keys based on hash function was generated wherein the generated frame key is consistent with the corresponding frame serial number which can ensure frame synchronization in the decrypting process can be achieved when frame loss occurs. This proposed algorithm provides security against some attack such as the frame regrouping attack and frame erasure attack and avoids the distribution of encryption keys. The results show that the proposed scheme was efficient in computing, the encryption process did not affect the compression ratio greatly, and the encryption/decryption process hardly affects the video quality.[9]

wang li-feng, wang wen-dong et al (2008): In wireless video applications, Security of video communication is important and challenging task. In this paper, the authors proposed the special feature of entropy coding on H.264 video which consist of coded block pattern permutation, sign of trailing ones scrambling and levels of nonzero coefficients encryption. The authors choose important syntax elements and sensitive coded elements using permutation and stream ciphers for an encryption. They have presented the experimental results which show that their proposed technique perceptual scheme can achieve high security at a relatively low compression ratio and bandwidth cost, as well as rather low complexity and time cost.[6]

III. CONCLUSIONS AND FUTURE WORK

With the increase of multimedia applications over the Internet, security of digital video information becomes more and more important. . In practice, digital video signals are often compressed before transmission and several video coding standards such as MPEG2, MPEG4, and H.264/AVC can be chosen for this purpose. These coding standards themselves do not provide any data encryption schemes. One early method is to apply an authentication control mechanism such that users are required to provide security information (e.g., password) before they can access the data. In the current work we have shown such a aspects for video encryption. In future we will present modified version of AES, with DWT as transformed domain for better video encryption.

IV. ACKNOWLEDGMENT

I am extremely grateful to the almighty god and my parents. I am thankful to Asstt. Prof. Kamaljeet kaur, ECE department, JMIT for her guidance and support.

REFERENCES

[1] Bing Zeng , Siu-Kei Au Yeung, Shuyuan Zhu and Moncef Gabbouj Perceptual Encryption of H.264 Videos: Embedding Sign-Flips Into the Integer-Based Transforms" *IEEE Trans. Inf. Security*,, vol. 9, no. 2,pp. 309–320, feb. 2014.

[2] Siu-Kei Au Yeung, Shuyuan Zhu, and Bing Zeng, Design of New Unitary Transforms for Perceptual Video Encryption" *IEEE Trans. Circuit Syst. Video Technol.*, vol. 21, no. 9, pp. 1341–1345, sept. 2011.

[3] Siu-Kei Au Yeung, Shuyuan Zhu and Bing Zeng, Partial Video Encryption Based on Alternating Transforms" IEEE. Signal proee,vol. 16, no. 10,pp.893-896, oct. 2009.

[4] Oi-Yan Lui, Kwok-Wo Wong, Chaos-based selective encryption for H.264/AVC"The journal of system and software86.,pp.3183-3192,2013.

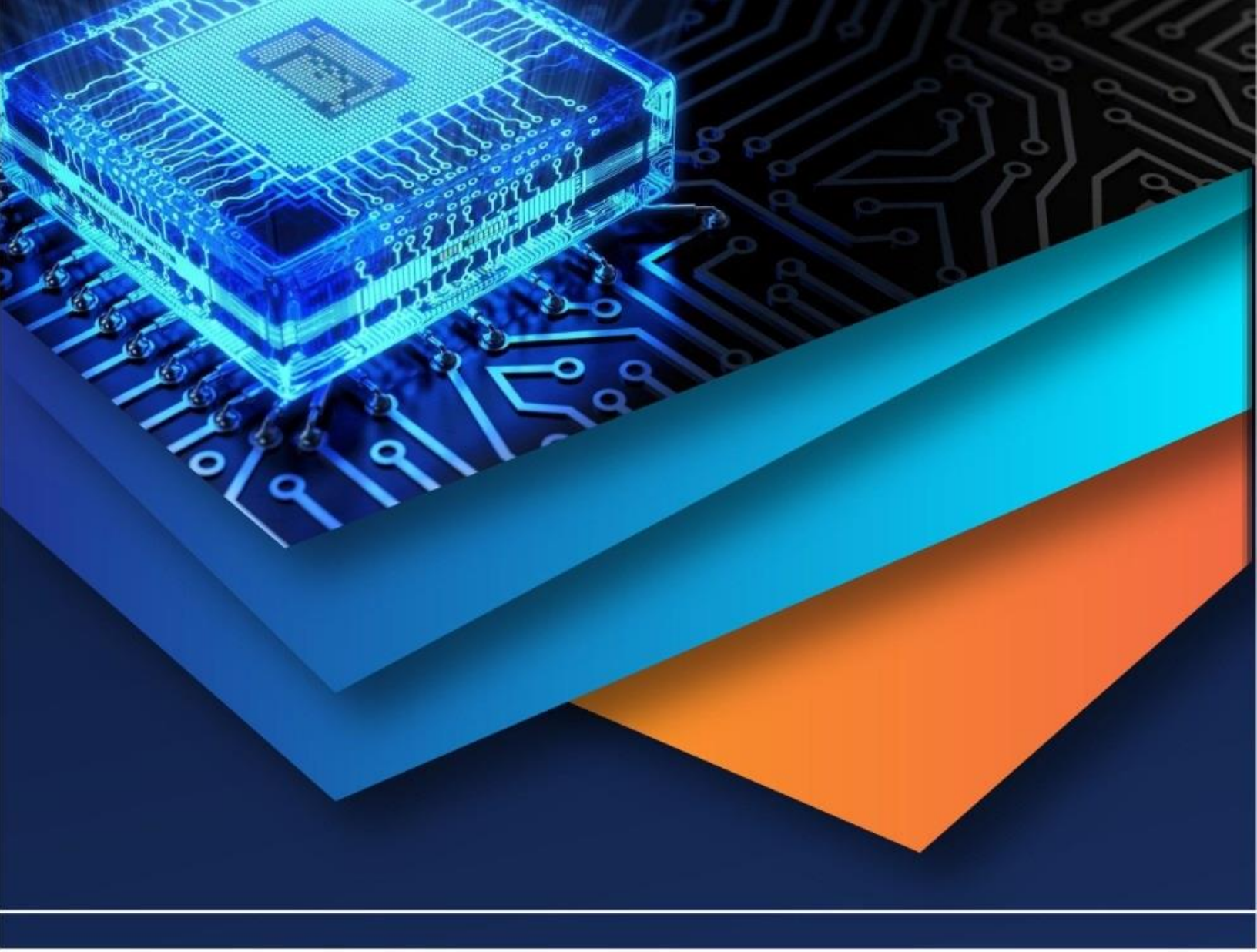
[5] Shiguo Lian , Xi Chen, On the design of partial encryption scheme for multimedia content" mathematical and computer modelling57,pp.2613-2624,2013.0

[6] WANG Li-feng, WANG Wen-dong, MA Jian, XIAO Chen, WANG Kong-qiao Perceptual video encryption scheme for mobile application based on H.264"science direct.pp.73-78,sept.2008.

[7] Gul Boztok Algin , E. Turhan Tunali " Scalable video encryption of H.264 SVC Codec" j.vis.commun.image R.22.pp.353-364,2011.

[8] Saeed Bahrami, Majid Naderi" Encryption of multimedia content in partial encryption scheme of DCT transform coefficients using a lightweight stream algorithm"optic124,pp.3693-3700,2013.

[9] Xiaofeng Wanga , Nanning Zheng , LihuaTian Hash key-based video encryption scheme for H.264/AVC" Signal Processing: Image Communication 25 .pp.427–437 ,2010.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY