Efficient Secret Data Sharing Using Multimedia Compression Paradigm

[1]E. Munuswamy, [2]M.Ferni ukrit
[1]Student,[2]Assistant Professor
[1]Department of Computer Science and Engineering
[1]DMI College of Engineering, Chennai, India

***Abstract* - In Early days, military commanders understood that it was necessary to provide some mechanism to protect the confidentiality of correspondence and to have some means of detecting tampering in statement. The existing system focuses on passing secret information by using steganography methodologies' secret text information is hided inside the video information in an encrypted form using the cryptographic key concept and passed to the receiver. The user in the receiving end has to take out the data using the cryptographic key in order to decrypt the information. The existing method concentrates on passing a secret information in the form text with the original video information. In the future system, any secret information in the type of text, image, audio, video has been hided in the original video information by the form of encoding and compression with the cryptographic key approach. Thus the proposed system has been checked for its originality of information at the receiver end by strong algorithmic concepts and the performance of the information security has been visualized graphically.**

***Index Terms* - Encryption, Compression ,Decompression, Decryption**

I.INTODUCTION

Network security which is defined as providing security for network by security policies and preventing from unauthorized access, misuse, modification of computer network and network-accessible resources. In recently, the Website security from the branch of Information Security, Network Security.. The term is generally used relating to computer networks, but is not partial to this ground; for example, it is also used in CPU resource organization. One common method of attack involve saturating the target machine with external connections needs, so much so that it cannot respond to legitimate traffic, the legitimate client also known as normal client ,the respond will be slow as to be rendered essentially unavailable. Such attacks usually causes to a server excess. Generally, DoS attacks are implement by either forcing the targeted computer(s) to reset, or utilize its resources so that it can no longer provide its intentional service or obstructing the communication media between the willing users and the victim so that they can no longer communicate adequately. The request overload prevents the resource from responding to legal traffic, or slows its response so significantly that it is rendered effectively unavailable. This situation is considered to be degradation situation or degradation of the machine or the system. This paper deals with data hiding in compressed video. different data hiding in images and raw video which operates on the images themselves in the spatial or transformed domain which are vulnerable to steganalysis, we goal the action vectors used to program and recreate both the forward predictive (P)-frame and bidirectional (B)-frames in compressed video. The selection of contestant division of these motion vectors are based on their associated macro block prediction error, which is diverse from the approach based on the motion vector attributes such as the size and phase angle, etc. A greedy adaptive threshold is search for every edge to get robustness while maintaining a low prediction error level. The secret communication bit stream is embedded in the least significant bit of both components of the applicant activity vectors. The method is implement and tested for hiding data in normal sequence of many groups of movies and the results are evaluated. The estimate is based on two criterion: minimum twist to the reconstruct video and least amount overhead on the compressed video size. Based on the abovementioned criteria, the proposed method is found to perform well and is compare to a action vector attribute-based method from the text.

II.LITERATURE SURVEY

[1].The main goal of this paper is to show how valuable is to perform log query taking out, by presenting several different applications of this idea combined with standard usage mining. In this we present two applications of the search train log. First, using the query distribution, we near an inverted file organization that has three levels: pre computed answers, main, and secondary memory indexes. Second, we present an algorithm that uses queries and clicks to improve ranking , which captures semantic relations of queries and Web pages.

[2].The data mining based on neural networks is research in detail. The key knowledge and ways to achieve the data mining based on neural networks are also discussed in this paper. Data mining process can be composed by three main phases like data research, data mining, expression and explanation of the results.

This paper only concentrated on mining processes and not in the transformation of data's extra functions of data.

[3].We provide a novel approach for clustering user-centric interests by analyzing tagging practices of individual users. The FCA(Formal concept analysis) and a significance measure is based on the weight of the tags in the given data set. The concept analysis technique makes it easy to mine common tags with respect to users in the data set**.**

It is not straightforward to build a general-level information for the given data.

We cant carry out the building of large community-level information's by adopting the approaches.

[4].Introduces a link-analysis procedure for discovering relationships in a relational database or a graph, generalize both simple and multiple communication analysis. It is based on a random-walk model from end to end the database defining a Markov chain having as many states as elements in the database.

The relational database could contain too many disconnected components, in which case our link analysis approach is almost useless

[5].Independent Software Vendors (ISVs) are now using virtual machines to deliver multiple software appliances. we present a performance evaluation framework for virtualized appliances. We also consider a range of different virtual machine configurations. **we** propose a complete security system for H.264/scalable video coding (SVC) video code and present a solution for the bit-rate and format compliance problems by careful selection of entropy coder syntax elements(bin-strings) for selective encryption (SE), and the problem of managing multiple layer encryption keys for scalable video.

production a slow change from non-overloaded to overloaded status.
The number of memory pages exchanged may not accurately represent the actual amount of data transferred
[6].An undesirable side effect of many watermarking and data-hiding schemes is that the host signal into which auxiliary data is embedded is distorted. Finding an best balance between the amount of in order embedded and the induced distortion is therefore an active field of research, there has been significant progress in understanding the basic limits of the capability versus distortion of watermarking and data-hiding schemes. For some application, however, no twist resulting from support data, however small, is allowed**.**

Optimal reversible data- hiding exploits the side information available from the received data.
[7].The use of robust watermarks to enable the characterization of attacks even after lossy compression, such as jpegand ijpeg2000**.** Previously constructed Bayesian framework is used to allow characterization of attacks from encoded files, and the double watermarking technique as earlier proposed by the authors is employed to generate the features used to drive the classified.
Increased computational complexity

[8]**.**The intra-prediction mode, motion vector difference and discrete cosine transform (DCT) coefficients' signs are encrypted, while DCT coefficients 'amplitudes are watermarked adaptively. To stay away from that the watermarking process affects the decryption process, a traditional watermarking algorithm is adapted. The encryption and watermarking operations are commutative. Thus, the watermark can be extract from the encrypted videos, and the encrypted videos be able to be re-watermarked.

The customized watermarking algorithm makes the watermarking action and encryption operation commutative.
It is high computational cost.

[9].Reversible data hiding has attracted more and more attention in both research and application. With reversible data hiding, at the statistics removal stage, both the original content and the hidden message be supposed to be completely extract, hence, how to design such scheme seem an attractive task. It can be secret into two brushwood, one is histogram-based system, and the other is perform by adjust the difference between nearby pixels.

a great deal additional data for reversible data hiding in comparison with conformist schemes.
[10].The first approach hides message bits by modulating the quantization scale of a constant bitratevideo. A payload of one message bit per macro hunk is achieved. A second order multivariate regression is used to find an association between macro block-level feature variables and the values of a hidden message bit. The regression copy is then used by the decoder to expect the values of the hidden message bits with very high prediction accuracy. The second approach uses the flexiblemacroblock ordering mark of H.264/AVC to hide meaning bits. Macro blocks are assign to arbitrary slice groups according to the content of the message bit to be hidden. A maximum load of three message bits per macro block is achieved.

III. METHODOLOGY

Rivest block cipher algorithm

In cryptography, Rc4 is the most generally used software stream cipher and is used in popular Internet protocols such as Transport Layer Security (TLS). While remarkable for its simplicity and speed in software, RC4 has weaknesses that disagree against its use in new systems. It is particularly weak when the beginning of the output key stream is not discarded, or when non-random or interrelated keys are used; some ways of using RC4 can lead to very insecure protocols such as WEP.

Huffman and byzantine algorithm

A Method for the Construction of Minimum-Redundancy Codes "The process of finding and/or by means of such a code is called Huffman coding and is a common technique in entropy encoding, with in lossless_data_compression. The algorithm's production can be viewed as a variable length code table for encoding a source symbol. Huffman's algorithm derives this table based on the estimated probability or frequency of occurrence (*weight*) for each probable value of the foundation mark.

The Byzantine Empire, alternatively known as the Eastern Roman domain, was the predominantly Greek-speaking eastern half continuation and remainder of the Roman__Empire during Late__Antiquity and the Middle__Ages. Its resources city was Constantinople the beginning founded as Byzantium. . During most of its existence, the realm was the most powerful economic, cultural, and military force in Europe. Both "Byzantine Empire" and "Eastern Roman Empire" are historiographical terms created after the end of the realm.

IV.SYSTEM MODEL

System model consist of the architecture diagram of the entire work. This explains clearly what the proposed system..the Architecture

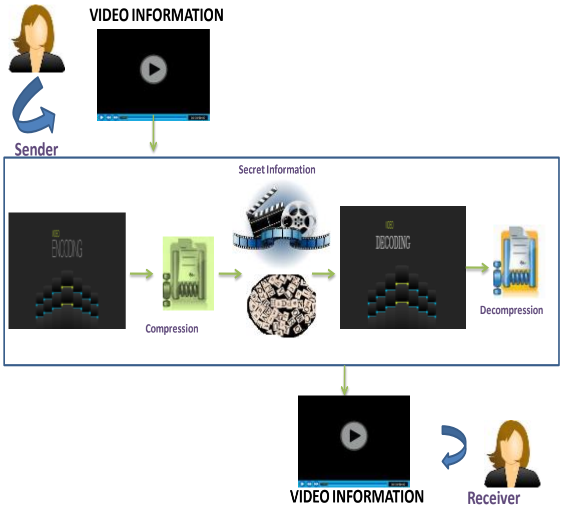


Diagram explain the overall process in this project to shown

Figure 1. Architecture Diagram

Sender

sender sends an information in the form of video using mp4 files to the receiver. It is also possible for the sender to send an hiding or secret information along with this video information. Sender sends video in encrypted form of information. Using encrypted form of content to ensure the confidentiality of inputs .Video file size is also strictly preserved while data embedding in a system.

Video information

Video information is acts as a input in this module. This Video information is stored and processed in an encrypted format. This encrypted form of video streams would avoid the leakage of the video content, which can help and address the security .Based on the encrypted format, original content privacy is protected. Data embedding and data extraction process also carried along with this video information. It is more efficient to meet the requirement of real time in this application.

Compression

Encrypted format of entire content is attain the next level that is compression of video information. To maintain the file size after encryption which requires that the impact on compression gain is minimal

Highly desirable to develop the algorithms that work entirely in an encrypted domain.

Using standard stream ciphers with encryption key to produce an encrypted video stream.

After, encryption original content is compressed along with the key generation

Decompression.

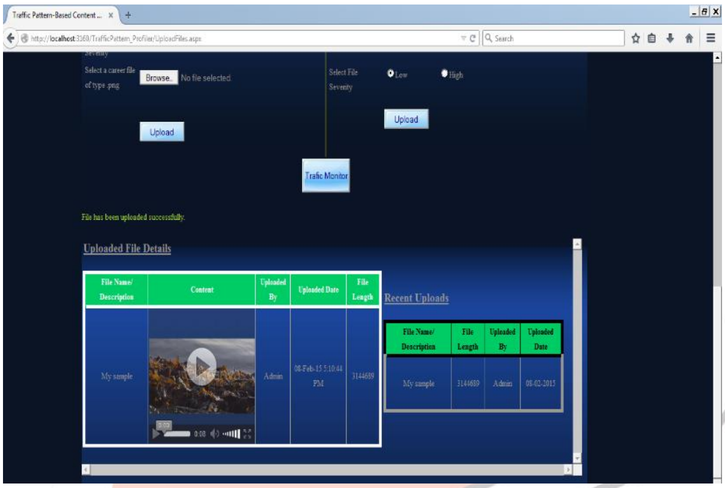
To protect privacy, a sender (e.g., cloud server) may only get access to the data hiding key and have to manipulate data in encrypted domain and this video information is changed into decompressed format. The visual quality degradation of decrypted video containing secret data is very low even for large payloads. Decoding of compressed content is generated along with secret source in a video files. Encrypted Cryptographic key helps to find out this secret data inside a video information .This decrypted of extract data is only able to view at the receiver end.

Receiver

When the user at the receiving end extract the secret data to ensure the confidentiality of the secret information along with this video. This secret information is viewed to receiver only when the codeword and length of decoded content matched with the database domain. Key is generated during decoding of original video data along with secret data. This key helps the receiver to view the secret source. The decrypted video still includes the hidden data, which can be used to trace the source of the video for the receiver. Receiver only makes sure about the confidentiality of data at the extraction end.

V. EXPERIMENTAL RESULTS AND DISCUSSIONS

The proposed methodology has been done in public. Here the Rc4 an algorithm is used for encryption and decryption. The compression process huffmanbyzantine algorithm is used.


Traffic Pattern-Based Content ...
http://localhost:3160/TrafficPattern_Profiler/UploadFiles.aspx
Search
Browse..
Upload
Upload
Trafic Monitor

Select a career file of type .png — No file selected

Select File Severity: ● Low ○ High

File has been uploaded successfully.

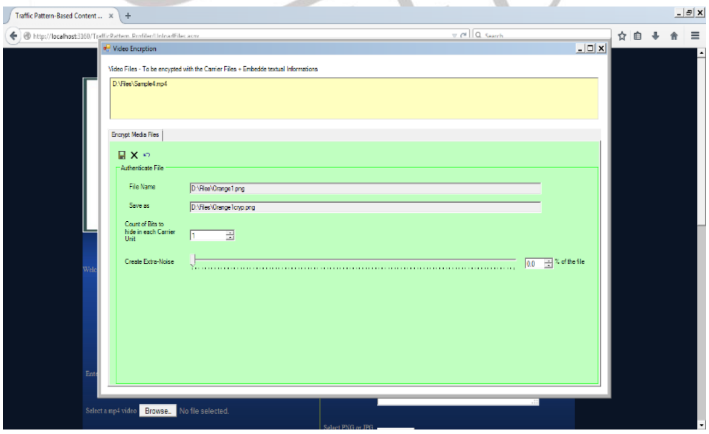
Uploaded File Details

File Name/ Description	Content	Uploaded By	Uploaded Date	File Length
My sample		Admin	08-Feb-15 5:10:44 PM	3144689

Recent Uploads

File Name/ Description	File Length	Uploaded By	Uploaded Date
My sample	3144689	Admin	08-02-2015

Figure 1. Video information


Traffic Pattern-Based Content ...
http://localhost:3160/TrafficPattern_Profiler/UploadFiles.aspx
Search
Video Encription
Encrypt Media Files
Browse..

Video Files - To be encypted with the Carrier Files + Embedde textual Informations

D:\Files\Sample4.mp4

Authenticate File

File Name: D:\Files\Orange1.png

Save as: D:\Files\Orange1cryp.png

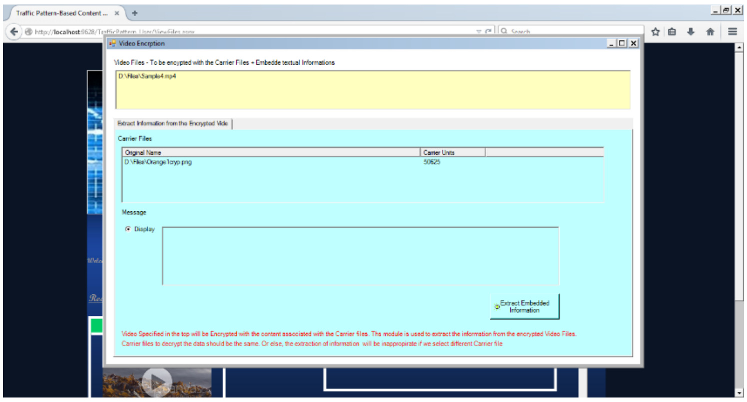
Count of Bits to hide in each Carrier Unit: 1

Create Extra-Noise: 0.0 % of the file

Select a mp4 video — No file selected.

Figure 2. Encryption information

Here the information will be hide and keys is provided by sender.. The manager provides key for decryption and the user decrypts the data from the receiver.



Traffic Pattern-Based Content ...

http://localhost:9628/TrafficPattern_User/ViewFiles.aspx

Video Encrption

Video Files - To be encypted with the Carrier Files + Embedde textual Informations

D:\Files\Sample4.mp4

Extract Information from the Encrypted Vide

Carrier Files

Original Name	Carrier Units
D:\Files\Orange1cryp.png	50625

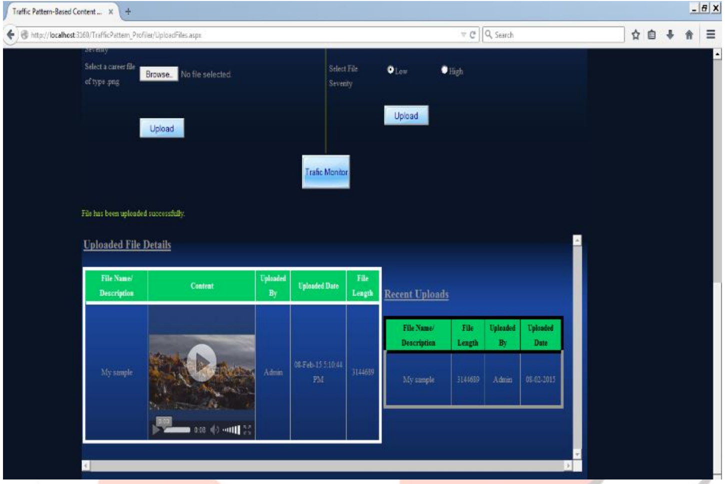
Message

● Display

Video Specified in the top will be Encrypted with the content associated with the Carrier files. This module is used to extract the information from the encrypted Video Files. Carrier files to decrypt the data should be the same. Or else, the extraction of information will be inappropirate if we select different Carrier file

Figure 3,Decryption information

In this fig the information wile is hide and also provided noise will be added to the original information to send to receiver.



Traffic Pattern-Based Content ...

http://localhost:3160/TrafficPattern_Profiler/UploadFiles.aspx

Select a career file of type .png Browse... No file selected

Select File Severity ● Low ○ High

File has been uploaded successfully.

Uploaded File Details

File Name/ Description	Content	Uploaded By	Uploaded Date	File Length
My sample		Admin	08-Feb-15 5:10:44 PM	3144689

Recent Uploads

File Name/ Description	File Length	Uploaded By	Uploaded Date
My sample	3144689	Admin	08-02-2015

Figure 4. Original video information

The video information stage decrypts the original content and will be seeing the receiver.

VI. CONCLUSION

Data concealing in encrypted media may be a new topic that has started to draw attention as a result of the privacy-preserving requirements from cloud information management. during this paper, an algorithm to engraft further information in encrypted H.264/AVC bit stream is given, that consists of video coding, data embedding and information extraction phases. Sender sends Associate in Nursing info within the sort of video exploitation mp4 files to the receiver. Rivest Block primarily based Ciphering algorithmic rule and information concealing in Encrypted H.264/AVC Video ,codeword substitution techniques concerned along and conceal the key content during this video supply. Encoded format of this content is compressed and also the compressed supply sends to the receiver**.**

REFERENCES

[1] P.K. Tysowski and M.A. Hasan, “Hybrid Attribute-Based Encryption and Re-Encryption for Scalable Mobile Applications in Clouds,” Technical Report 13, Centre for Applied Cryptographic Research (CACR), Univ. of Waterloo, 2013.

[2] R.L. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” Comm. ACM, vol. 26, no. 1, pp. 96-99, Jan. 1983.

[3] N. Balasubramanian, A. Balasubramanian, and A. Venkataramani, “Energy Consumption in Mobile Phones: A Measurement Study and Implications for Network Applications,” Proc. Ninth ACM SIGCOMM Conf. Internet Measurement Conf. (IMC ’09), pp. 280-293, 2009.

[4] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-Policy Attribute-Based Encryption,” Proc. IEEE Symp. Security and Privacy (SP ’07), pp. 321-334, 2007.

[5] A. Tassanaviboon and G. Gong, “OAuth and ABE Based Authorization in Semi-Trusted Cloud Computing: Aauth,” Proc. Second Int’l Workshop Data Intensive Computing in the Clouds (DataCloud-SC ’11), pp. 41-50, 2011.

[6] X. Liang, R. Lu, and X. Lin, “Ciphertext Policy Attribute Based Encryption with Efficient Revocation,” Technical Report BBCR, Univ. of Waterloo, 2011.

[7] J. Hur and D.K. Noh, “Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems,” IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214-1221, July 2011.

[8] G. Zhao, C. Rong, J. Li, F. Zhang, and Y. Tang, “Trusted Data Sharing over Untrusted Cloud Storage Providers,” Proc. IEEE Second Int’l Conf. Cloud Computing Technology and Science (CLOUDCOM ’10), pp. 97-103, 2010.

[9] P.K. Tysowski and M.A. Hasan, “Towards Secure Communication for Highly Scalable Mobile Applications in Cloud Computing Systems,” Technical Report 33, Centre for Applied Cryptographic Research (CACR), Univ. of Waterloo, 2011.

[10] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, “Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage,” ACM Trans. Information and System Security, vol. 9, pp. 1-30, Feb. 2006.

[11] S. Jahid, P. Mittal, and N. Borisov, “EASiER: Encryption-Based Access Control in Social Networks with Efficient Revocation,” Proc. Sixth ACM Symp. Information, Computer and Comm. Security (ASIACCS ’11), pp. 411-415, 2011.

[12] Q. Liu, G. Wang, and J. Wu, “Clock-Based Proxy Re-Encryption Scheme in Unreliable Clouds,” Proc. 41st Int’l Conf. Parallel Processing Workshops (ICPPW), pp. 304-305, Sept. 2012.

[13] J.-M. Do, Y.-J. Song, and N. Park, “Attribute Based Proxy Re- Encryption for Data Confidentiality in Cloud Computing Environments,” Proc. First ACIS/JNU Int’l Conf. Computers, Networks, Systems and Industrial Eng. (CNSI), pp. 248-251, May 2011.

[14] S. Yu, C. Wang, K. Ren, and W. Lou, “Attribute Based Data Sharing with Attribute Revocation,” Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS ’10), pp. 261-270, 2010.

[15] Y. Ming, L. Fan, H. Jing-Li, and W. Zhao-Li, “An Efficient Attribute Based Encryption Scheme with Revocation for Out- sourced Data Sharing Control,” Proc. First Int’l Conf. Instrumentation, Measurement, Computer, Comm. and Control, pp. 516-520, 2011.

[16] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing,” Proc. IEEE INFOCOM ’10, pp. 534-542, 2010.

[17] K. Yang and X. Jia, “Attributed-Based Access Control for Multi- Authority Systems in Cloud Storage,” Proc. IEEE 32nd Int’l Conf. Distributed Computing Systems (ICDCS), pp. 536-545, 2012.

[18] K. Yang, X. Jia, K. Ren, and B. Zhang, “DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems,” Proc. IEEE INFOCOM, pp. 2895-2903, 2013.

[19] J. Wang, “Java Realization for Ciphertext-Policy Attribute-Based Encryption,” http://github.com/wakemecn, 2012.

[20] G. Wang, Q. Liu, and J. Wu, “Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services,” Proc. 17th ACM Conf. Computer and Comm. Security (CCS ’10), pp. 735-737, 2010.