REDUCTION OF TRAFFIC AND DELIVERY OF VIDEO IN TO THE TRUSTED NETWORK USING QUICK RESPONSE CODE

[1]Nivetha. R, [2]T.SheikYousuf
[1]PG Scholar, Department of Computer Science and Engineering, Mohamed Sathak Engineering College,
Ramanathapuram, India.
[2]Assistant professor, Department of Computer Science and Engineering, Mohamed Sathak Engineering College,
Ramanathapuram, India
[1]nivetha074@gmail.com, [2] sheikres@gmail.com

Abstract: The real-time video streaming applications and services over the Internet has increased in recent years. This project focuses on the illegal redistribution of streaming content by an authorized user to external networks. It sends streaming content by an authorized user to external networks. The tiff format is used for sending the video streaming from the client to server. The videos are converted into frames. After that the frames are modified into the image frame where one tiff file having a number of images within it. Then this image frame is added to the QR (Quick Response) code. A QR code is a type of 2D bar code that is used to provide easy access to information through the network. This tiff files are send through the QR code from the sender to the receiver**.**

Keywords: Streaming, Tiff format, Quick Response code, 2d bar code.

1. INTRODUCTION

Streaming content is an audio or video file on the Internet that is partially downloaded and then played as the remainder of the file is being downloaded. Video streaming is the method of constantly sending and receiving content over the Internet. Streaming media are beneficial in that they significantly reduce wait times for online content; usually depending on the speed of their connection. Online radio stations and YouTube videos are both good examples of streaming content. While streaming audio is not quite as bandwidth-intensive, streaming video require more bandwidth [3]. If User wants to view streaming movies should have an Internet speed of at least 2.5 Megabits per second. For high definition content, 10 Mbit/sec is recommended. Streaming video is content send in compressed form over the Internet and displayed by the viewer in real time. For streaming video or streaming media, a Web user needs not to wait to download a file. The media is sent in a continuous stream of data and is played as it arrives. Content based detection“Content-based” means that the search analyzes the contents of the image rather than the metadata such as keywords, descriptions associated with the image. The term "content" is refer to colors, shapes,or any other information that can be derived from the image itself. CBIR is also known as query by image content (QBIC) and content-based visual information retrieval (CBVIR) is the application of computer vision techniques to the image retrieval problem[5].The problem of searching for digital images in large databases desirable because searches that purely on metadata are dependent on annotation quality and completeness. Having humans manually annotate images by entering keywords or metadata in a large database can be time consuming and maynot capture the keywords desired to describe the image. The evaluation of the effectiveness of keyword image search is subjective and has not been well-defined.

2. RELATED WORKS

2.1 Content Leakage Detection

Typical Video Leakage Scheme due to the popularity of streaming distribution of movies, improvement of P2P emerging software has attracted much attention. These technologies augment the distribution of any type of information over the Internet. A regular user in a secure network receives streaming content from a content server. After, with the use of a P2P streaming software, the regular malicious users redistributes the streaming content to a non-usual user outside its network. Such content-leakage is hardly hit-upon or blocked by watermarking and DRM based techniques [4]. Throughout the video streaming process, the changes in the amount of traffic appear as a unique waveform of specific to the content. By critique this propaganda retrieved at different nodes in the network, content-leakage can be detected. An urge of the network topology of the proposed leakage detection system is shown in figure. This topography consists of two central components, namely the traffic pattern generation engine embedded in individual router, and the traffic pattern matching engine implemented in the enabled server. Thus, each router can observe its traffic volume and generate traffic pattern [2].

The traffic pattern generation process is executed in conventional methods. Traffic pattern generation process is situated on either time slot-based algorithm or packet size-based algorithm. Thus traffic pattern provoked, is expressed as an N-dimension vector as follows:

$$X^N = (x1 ,x2,\ldots,x^N)^T$$

Where xi indicates the volume of the ith chunk, and N is the number of chunks [6]. Time slot-based algorithm is a undisguised solution to generate traffic patterns by summing the amount of traffic arrival during a certain period of time. In case some packets are delayed, they may be gathered over the following slot, x1, instead of the primary slot, xi[10]. Therefore, delay and jitter of packets distorts the traffic pattern, and as a consequence, downturn the accuracy in pattern matching. In figure 2 traffic pattern generation process for each packet size.

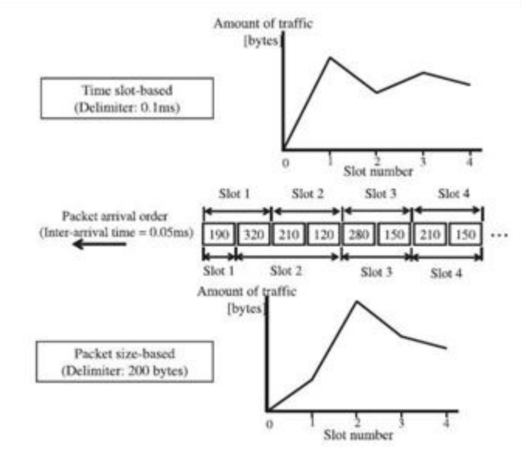

Amount of traffic [bytes]
Time slot-based (Delimiter: 0.1ms)
0
1
2
3
4
Slot number
Slot 1
Slot 2
Slot 3
Slot 4
Packet arrival order (Inter-arrival time = 0.05ms)
190
320
210
120
280
150
210
150
...
Slot 1
Slot 2
Slot 3
Slot 4
Amount of traffic [bytes]
Packet size-based (Delimiter: 200 bytes)
0
1
2
3
4
Slot number

Figure 1: Traffic Pattern Generation Process

2.2 Pattern Matching Algorithm

In pattern recognition, the degree of relationship is defined to be the parallel measure in between the patterns. The server-side traffic patterns represents the authentic traffic pattern and is expressed as

$$X^S =(x1, x2, . . .x^s)^t$$

The user-side traffic pattern is defined and then window is then moved from left to right by one slot. These three steps are repeated continuously till the window reaches the rightmost part of the server-side pattern. Thus it need to obtain (S -U + 1) values of similarities. However, the existence of videos of different lengths subjected to time variation in real content delivery environment causes DP-TRAT's accuracy to decrease[9].While focusing on DP-TRAT, introduces a new threshold determination method based on an exponential approximation and evaluate the computation cost of both the proposed scheme and an eventual enhancement of the previous scheme [3].

2.3 Different Lengths of Videos

Traffic patterns of cascade videos represent the skeleton carrying their characteristics and are exclusive per content. Therefore, the longer the traffic pattern is, the more detailed on the video that are falsified. In conventional methods, it is considered that a certain length of content can always be achieved through the network for all ladings. Therefore, it is possible to use a fixed decision threshold in both P-TRAT and DP-TRAT methods. There are no such assured in actual network environments. It shows an instance of the occurrence of an erroneous decision in a network environment with different length of videos. The conventional approaches, namely, time slot-based traitor tracing (T-TRAT), packet size-based traitor tracing (P-TRAT) and DP-based traitor tracing (DP-TRAT), based on the aforementioned algorithms are complied.

The time slot-based pattern generation algorithm used in T-TRAT is altered by packet delay and jitter, which degrade the user-side traffic pattern. On the other hand P-TRAT and DP-TRAT utilizes a traffic pattern generation method based on packet size rather than time slot. As a result, P-TRAT and DPTRAT shows robustness against packet delay and jitter. Meantime, DP matching dynamically alleviates this issue and shows high robustness to variation in network environment such as the occurrence of packet loss[3]. The determination of the predefined decision threshold used in P-TRAT and DP-TRAT is depicted in Figurer by computing the median between the degree of similarity resulting from the comparison with the same video and the maximum value of the degree of similarity resulting from the comparison with different videos.

2.4 Traffic pattern generation process

The packet filtering by firewall-equipped egress nodes is an easy solution to avoid leakage of streaming contents to exterior networks. In this solution, the packet header information) of every streamed packet is inspected. However, it is difficult to entirely prevent streaming content leakage by means of packet filtering alone because the packet header information of malicious users is unspecified beforehand and can be easily spoofed. The illegal redistribution of streaming content by an authorized user to external networks. The existing proposals in monitor information obtained at different nodes in the medial of the streaming path. The rescued information are used to generate traffic patterns which appear as unique waveform per content just like a fingerprint.

3. PROPOSED WORK

In proposed system, handling the network traffic with the coding techniques for securely send and receive the traffic. In existing system the drawback of network traffic and it’s distributing the bottleneck at the time of transmission. To overcome the problems faced in the existing system have to move on to the security based QR technique [6]. In proposed system sending the video streaming content by an authorized user to external networks. Here, the tiff format is used for sending the video streaming from the client to server. In that the video can be divided into the frame and it can convert into the tiff image, where tiff file having a number of images within it. Then this image frame is added to the QR code (quick response code).

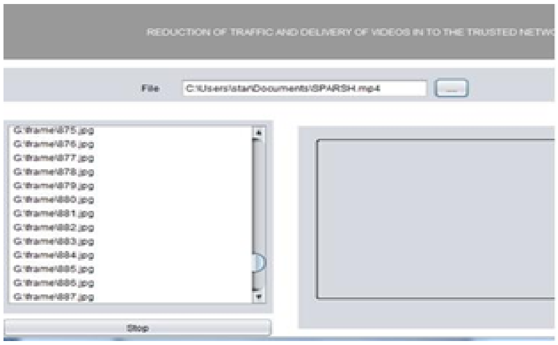
A QR code is a type of 2D bar code that is used to provide easy access to information through the network. This tiff files are send through the QR code from the sender to the receiver. Here it can easily find out the leakage or data loss when the message is received to the destination. Then the information stored as secure information in the tiff file and can decrypted or restored at the user-side by authorized yet malicious users. In figure 1 video conversion to an frames is shown The results show that the QR increases the performance of the network when the video streaming can be performed. The QR code is much faster than the barcode. Then the delay of the network is also reduced by our proposed QR code. The process behind is to change the frames into images. The images are in tiff format. The judgment for selection of tiff format is to reduce the size. The frames are converted into some type of image. For that the frames are combined and changed into tiff format. The purpose of converting the tiff file is to reduce the size of the video. In video transmission process each and every process of the QR code must to be transmitting. Because every file in the QR code could be translated code using some other processes. The before enrichment of transmission the files in the client side or server side it can be transmitted into opponent side [5]. The way of constructing these processes have to increase the time of secure data transmission.

The result of the overall process can deliver the result of consumption of data loss at the time of data transfer. The QR code could be disparately ensuring the security of every files in the list. At the end of receiver side the translated file can be viewed by them and it can be in the form of secured manner and without any data loss. As a result, the process of QR code is usually encoded and also decodes the process of every file.

3.1 Conversion

The first process of our concept is to choose a video file for processing. Here, take the mp4 based file format. This video file can be loaded and it can be converted into frames. The division of frames is based on the size of the video file. According to the frame conversion move on to next stage. At the time of video to frames conversion the size of the video file to be increase. To reduce the size of the converted file move onto the tiff image conversion.

To overcome the problems faced in the existing system we have to move on to the security based OR technique. In proposed system we are sending the video streaming content by an authorized user to external. The similarity of traffic patterns were calculated by the cross-correlation matching algorithm in the matching process. Another pattern matching algorithm was the dynamic programming (DP) matching based on the DP technique. Finally, the existing system compared the adjusted degree of similarity to the decision threshold specific to the primitive video, and recognizes whether or not there is a leakage.



REDUCTION OF TRAFFIC AND DELIVERY OF VIDEOS IN TO THE TRUSTED NETWO

File C:\Users\star\Documents\SPARSH.mp4

G:\frame\875.jpg
G:\frame\876.jpg
G:\frame\877.jpg
G:\frame\878.jpg
G:\frame\879.jpg
G:\frame\880.jpg
G:\frame\881.jpg
G:\frame\882.jpg
G:\frame\883.jpg
G:\frame\884.jpg
G:\frame\885.jpg
G:\frame\886.jpg
G:\frame\887.jpg

Figure 2: Selecting videos for conversion to TIFF images

3.2 TIFF image

The TIFF (Tagged Image File Format) format is a flexible format that normally saves 8 bits or 16 bits per color (red, green, blue) for 24-bit and 48-bits. Usually using each of the the TIFF or TIF filename extension. The tagged structure was illuminate to be easily extendible, and many vendors have introduced recovery special-purpose tags – with the result that no reader handles every flavor of TIFF file TIFFs can be lossy and lossless some offer equally good lossless compression for bi-level (black & white) images. Some digital cameras can save images in TIFF format, using LZW compression algorithm for lossless storage. TIFF image format is not generally supported by web browsers. TIFF remains to be accepted as a photograph file standard in the printing business. TIFF can handle device in a specific color spaces, like the CMYK defined by a particular set of printing press inks. OCR (Optical Character Recognition) software packages commonly generate some form of TIFF image (often monochromatic) for scanned text pages. Figure shows conversion of frames into a tiff images.

Figure 3: Videos are converted to tiff images

3.3 Quick response code

QR code (quick response code) is a type of 2D bar code that is used to provide easy access to information through a Smartphone. Static QR codes, the most common type, are used to diffusion information to the general public. They are often displayed in promoting materials in the environment, on television and in newspapers and magazines. The code's designer can track information about the number of times a code was scanned .The associated action taken, along with the times of scans and the operating system of the devices that scanned it.

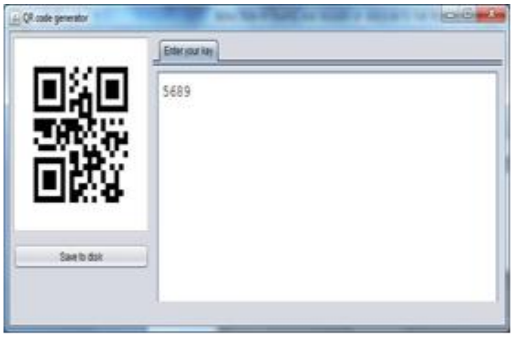
Dynamic QR codes (unique QR codes) offer more functionality. The Possessor can edit the code at any time and can target a specific individual for personalized marketing. Such codes can track more particular information, with the scanners names and email address, many times they scanned the code and in conjunction with tracking codes on a website, conversion rates. The QR Code system has become popular outside the automotive industry due to its fast readability and greater storage capacity compared to standard UPC barcodes. Applications include device tracking, product identification, time tracking, document management, and many.

QR code consists of black modules (square dots) arranged in a square grid on a white background, which can be read by an imaging device (such as a camera) and processed using Read–Solomon error correction until the image can be appropriately interpreted. The enforced data are then selected from patterns present in both horizontal and vertical components of the image. QR codes can be used in Android, BlackBerry OS, Apple devices, Microsoft Windows Phone, Google, 3rd party barcode scanners, and the 3DS. These devices support URL retraction, which allows QR codes to send metadata to existing applications on the device. The barcode is a QR code reader for the operating system. In Apple's IOS and Android, a QR code reader is not included, but cost and free apps are available with both the ability to scan the codes and hard-link to an external URL. BlackBerry 10 devices have a QR reader as well as several third party readers. Windows Phone devices can scan QR codes with Bing Vision.

Although initially used to track parts in vehicle manufacture, QR codes are now used over a much expanded range of applications, including crucial tracking, entertainment and transport ticketing, loyalty marketing and store product labeling. It can also be used in accumulate personal information for use by organizations. Users may receive text, add a vCard contact to their device, open a Uniform Resource Identifier (URI), or compose an e-mail or text message after scanning QR codes. They can achieve and print their own QR codes for others to scan and use by visiting one of several pay or free QR code-generating sites or apps. Google had a popular API to achieve QR codes and apps for scanning QR codes can be found on nearly all smart phone devices. QR codes storing addresses and Uniform Resource Locators (URLs) may appear in magazines,on business cards, or on at most any object about which users might want information.

Users with a camera phone equipped with the correct reader application can scan the image of the QR code to display text, establish a connection to a wireless network, and otherwise open a web page in the telephone's browser. This process of linking from physical world objects is termed hard linking or objects hyper linking. QR codes also may be linked to a location to track where a code has been scanned. whether the application that scans the QR code derive the geo information by using GPS and cell tower triangulation (aGPS) or the URL encoded in the QR code itself is associated with a location QR codes can be used to store bank account information or credit card information, or they can be definitely designed to work with distinct payment provider applications.

QR codes are commonly used in the field of cryptographic currencies, notably those based off,along with Bitcoin. Payment detail, cryptographic keys and transaction information are often shared between digital wallets in this way. This tiff files are send through the QR code from the sender to the receiver. Here simply find out the leakage or data loss when the message is received to the destination. In figure 4 QR code are generated with an security code from frames.



5689

Figure 4: QR code is generated with security code

3.4 Decryption Process

Every file in the QR code could be transformed to some other code using some other processes. The before enrichment of transmission the files in the client side or server side it can be transmitted into opponent side. The way of constructing these processes we have to increase the time of secure data transmission. The result of the overall process can deliver the result of consumption of data loss at the time of data transmission. Then the QR code could be separately arranging the security of every file in list. At the end of receiver side the transmitted file can be viewed by them and it can be in the form of secured manner and without any data loss. Because the process of QR code is frequently encode and also decode the process of every file. These images having a particular order to rearrange, Sender can send this image and that rearranging order to the receiver. Receiver can decrypt the images and watch the video without delay

4. SYSTEM FLOW DIAGRAM

In Figure 5 System diagram for sending secure video to a receiver. The first process of our concept is to choose a video file for processing. This video file can be loaded and it can be converted into frames. To minimize the sizes of the converted file have to move onto the tiff image conversion. Than QR code is generated for security purposes. Video are transmitted they are decrypted with security code through mail.

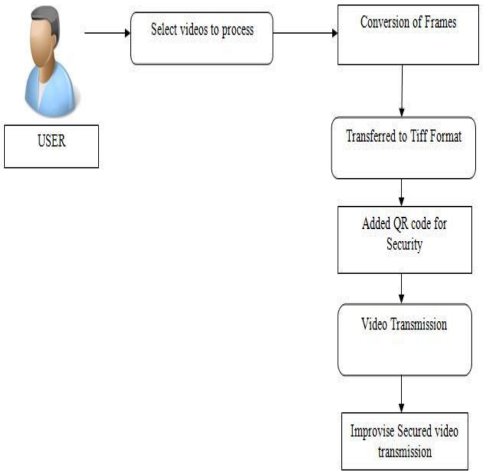

USER
Select videos to process
Conversion of Frames
Transferred to Tiff Format
Added QR code for Security
Video Transmission
Improvise Secured video transmission

Figure 5: System Flow Diagram

5. CONCLUSION AND FUTURE WORK

5.1 Conclusion

The content leakage find system based on the fact that each streaming content has a unique traffic pattern is an innovative solution to prevent illegal redistribution of contents by a regular, yet malicious user. In this proposed system it can achieving the efficient video transmission by converting into frames and that frames are converted into tiff images for reducing the traffic. QR is used to send these images in a secure way. These kinds of security policies are generating a bar code for transmission process. The tiff files and QR code send from the source to destination. QR code is easily retrieving the original data, so it can be increase the system performance and reduce the network delay.

5.2 Future Enhancement

In proposed work, multimedia streaming application there is a possibility of content leakage. To prevent this leakage we must securely transmit the videos into the streaming path. To convert the videos into frames, after that frames are modified into the image frame. These image frames are added to the QR code and send to the receiver. In receiver side, use the QR code to decrypt the messages and then seen. Improvising these techniques by renewal the video Steganography. The preferences of Steganography over Cryptography alone are that the intended secret message does not attract attention to itself as an object of scrutiny. In multimedia transmission, stegnography is the best way of encryption because of video file size is larger when compared to the document.

6. ACKNOWLEDGEMENT

Author like to thank the respective Head of the Institution, Head of the Department and Faculty members for giving valuable advices and providing technical support.

REFERENCES

[1] Z. Yang, H. Ma, and J. Zhang, “A Dynamic Scalable Service Model for SIP-Based Video Conference,” Proc. Ninth Int’l Conf. Computer Supported Cooperative Work in DE, pp. 594-599, May 2005.

[2] Y. Chu, S.G. Rao, S. Seshan, and H. Zhang, “Enabling Conferencing Applications on the Internet Using an Overlay Multicast Architecture,” Proc. ACM SIGCOMM, 55-67, Aug. 2001.

[3] O. Adeyinka, “Analysis of IPSec VPNs Performance in a Multimedia Environment,” Proc. Fourth Int’l Conf. Intelligent Environments, pp. 25-30, 2008.

[4] K. Su, D. Kundur, and D. Hatzinakos, “Statistical Invisibility for Collusion-Resistant Digital Video Watermarking,” IEEE Trans. Multimedia, vol. 7, no. 1, 43-51, Feb. 2005.

[5] Y. Liu, Y. Guo, and C. Liang, “A Survey on Peer-to-Peer Video Streaming Systems,” Peer-to-Peer Networking and Applications, vol. 1, no. 1, pp. 18-28, Mar. 2008.

[6] M. Dobashi, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour, “Traitor Tracing Technology of Streaming Contents Delivery Using Traffic Pattern in Wired/Wireless Environments,” Proc. IEEE Global Telecomm. Conf., pp. 1-5, Nov./Dec. 2006.

[7] A. Asano, H. Nishiyama, and N. Kato, “The Effect of Packet Reordering and Encrypted Traffic on Streaming Content Leakage Detection (Invited Paper),” Proc. Int’l Conf. Computer Comm. Networks (ICCCN ’10), pp. 1-6, Aug. 2010.

[8] S. Amarasing and M. Lertwatechakul, “The Study of Streaming Traffic Behavior,” KKU Eng. J., vol. 33, no. 5, pp. 541-553, Sept./ Oct. 2006.

[9] Y. Gotoh, K. Suzuki, T. Yoshihisa, H. Taniguchi, and M.Kanazawa, “Evaluation of P2P Streaming Systems for Webcast,”Proc. Sixth Int’l Conf. Digital Information Management, pp. 343-350, Sept. 2011.

[10] Y. Zhang, P. Ma, and X. Su, “Pattern Recognition Using Interval-Valued Intuitionistic Fuzzy Set and Its Similarity Degree,” Proc. IEEE Int’l Conf. Intelligent Computing and Intelligent Systems, pp. 361-365, 2009.

[11] E. Diehl and T. Furon, “Watermark: Closing the Analog Hole,”Proc. IEEE Int’l Conf. Consumer Electronics, pp. 52-53, 2003.

[12] Y. Liu, Y. Guo, and C. Liang, “A Survey on Peer-to-Peer Video Streaming Systems,” Peer-to-Peer Networking and Applications, vol. 1, no. 1, pp. 18-28, Mar. 2008.

[13] E.D. Zwicky, S. Cooper, and D.B. Chapman, “Building Internet Firewalls”, second ed., O’Reilly and Assoc., 2000