

Streaming Secured Layer Media using IP Network Sharing

Abstract:

Imagine that you are a student at Stevens Institute of Technology and you are informed that school is closed due to inclement weather. What this means is that you miss school lectures which are valuable to your success as a professional engineer. It is about three days before you are able to attend classes and much time will be needed to catch up on your course work.

The professor informs the class that he will have to increase the pace of the lectures to cover the missed material. As a result you and other students go to administration to complain about the conditions creating this extra work load. The administration listens and has research conducted to find out ways to correct the problem just in case the weather condition is a factor in the future for school cancellations.

The Computer Engineering department acquires three students as a research project to find out a way to distribute lectures to the class in a secure environment and manner. The three students realize that watermarking is the key to this solution, but now they must determine the method that is best for the institution.

Each lecturing professor will present their lectures and have them recorded by video camera, which will capture both video and audio. The audio and video will be captured from the analog source and converted into digital format. Once the source has been converted, the data will be sampled at different rates for use in variable bandwidth environments.

Once sampled, the lectures will be made available on the Stevens network for all students stream, and also it will be available for students to connect through a secure server. In addition to this the student will have the option to download the files to listen to on the local hard drive if connection to the Internet is a problem. Stevens administration likes the idea but is worried about copyright infringements. Thus you inform them that watermarking methods will help to place ownership on each file and so Stevens can prove legal it is their property.

To prove that it works, you simulate the Stevens environment using IP Network sharing which allows you to have multiple IPs from only one. You show the streaming for them and the security of the content being accessed. You get an

'A' for you hard work and some duck bills. Now Stevens can not only distribute to full time students, but they can sell Lectures to student that want an education without being physically in the classroom, and it is made possible by placing ownership in all the information distributed.

Project Proposal Plan

Introduction:

As technology has evolved allowing mass storage of information, the issue of protecting intellectual property has become a big problem. How do you protect your intellectual property as an institution or as an individual? The answer to this question is the use of a watermark, also known as a copyright label or digital signature. Watermarking is a technique of marking digitally stored data in such a way that ownership can easily be established.

The best watermarks are constructed using a random generator, since most noise is of a random nature. By statistical analysis the best random generator is a Gaussian generator. This means that Gaussian noise is the most difficult pattern to detect. Therefore a Gaussian random generator was used to create the watermark used in our demonstration. For audio files, such as in this design project, a watermark is a vector whose elements have a mean of zero with a variance of one. This design project will cover only basic watermarking concepts and basic techniques. But there are many ways to mark data with a watermark.

To make sure that we cover all the issues with an advance network environment we want to show how multiple users would access the same file through several host computers. This will be made possible by design a special network that allows you to access up to 253 IP with only one source IP, using IP masking techniques. Special routers with built firewalls will allow this to take place. Because of this new method to distribute the information we have to have a medium by which students can access it.

All watermarking will be applied to .wav file formats which is the parent type from which all the newest formats are generated including the newest and most controversial .mp3 (Layer III) format. We will insert the watermark and then take the .wav file and compress it to .asf, .rm, .mp3, and .wma formats which will be audio files. We will extract the .wav format from an .avi file, insert the watermark and then interweave the .avi file again. Then we have ownership for .avi which is the parent format for all video applications. We can then compress the .avi into .asf, .rm, mpeg-4, quick time .mov formats to show how the watermarking techniques work in the compressed environment.

IP Address sharing is an excellent and cheap solution to the limited Ethernet jack problem that Stevens will face upon the implementation of a new multimedia streaming applications system. It will provide fast and easy connection to the network for a broad range of new and incoming students that purchase laptops, as a requirement, upon their acceptance to the school. As a greater number of users require connectivity, IP Address sharing will play an even greater role in servicing larger numbers of nodes due to its easy scalability.

Design Requirements:

Students who miss their classes because of on-campus events such as interviews, appointments, or extracurricular activities can listen to, and view, the lectures that they've missed at their leisure or during their free time between those activities. The use of IP (Internet Protocol) Address Sharing can help achieve a service that is fast and reliable similar to that used now outside of the Student Service Center enabling one to view personal information. The problem with the implementation of the current system is that it allows only one user at a time to view information. That is, there are three terminals that would allow one user, per terminal, to view their account status.

In order to allow more people to simultaneously use the service, more kiosks would have to be purchased and network upgrades would have to be completed. However, with the use of IP Address sharing, Stevens would not need to supply computer terminals, hence, saving money. Implementing an IP Address sharing scheme would require as little as a single routing device, attached to one RJ45 jack, configured as a DHCP server. With this configuration, as many as 253 simultaneous users can connect to the web or internal campus network and view their account status information as well as multimedia streaming files from the multimedia applications system. In addition to providing connectivity to a large number of users, IP Address sharing grants excellent security to those attached to the network. The very nature of name-address-translation, the technology beneath IP Address sharing that makes it all possible, fundamentally provides a firewall to all connected nodes.

Without some sort of address routing device or software, a network composed of 253 clients and a single server would have problems upon a client's request for Internet data packets. Say that the network in question configured in a star topology with a 300 port hub and that all the network IP addresses are dynamically assigned to the nodes by the server upon their boot up. In such a situation, the server may be configured to consider the nodes in that one

particular hub as a subnet, say 255.255.255.0, and therefore may assign an IP address ranging from X.Y.Z.0 to X.Y.Z.254. This is all will work for file and printer sharing among the nodes given that they have shared drives and printing devices, however, it will not allow any one node to successfully leave the Stevens network. Nodes that try to access external networks like the Internet would find themselves sending out URL (Universal Resource Locator) requests to the server without a response.

Two things may happen: One, the server may not know what to do with the URL and may ignore the request from the node. Or two, the server may go actually go as far as contacting a DNS (Domain Name Server) for the web page, but, upon receipt of external packets, will not know what node on the star network to send the data to. With a routing device, packets sent to the server by a node will be picked up and examined by the device. After logging the sender's address, the routing device sends the URL to the default DNS. Once the IP address is found, the web page will be accessed data will return to the routing device. Upon receipt of the information, it will correctly send the packets to the initiating node through the hub. These routing devices internally build tables containing client IP and MAC (Media Access Control) addresses from proper packet routing.

In essence, we would like to provide Stevens with a solution to Ethernet jack "gridlock". The RJ45 ports that have already been installed in several Stevens rooms will become essential and will be in high demand by the students. Hence, 4 or 5 jacks per room will not suit the student body's needs any longer. Instead of having to install more RJ45 jacks per room, one routing device can be connected to each Ethernet port already present without causing any conflict. Stevens DHCP servers would treat the devices as a regular laptops attached to an RJ45 jack and would supply a network safe IP. With such a setup, the number of users could increase to $x \cdot 253$ where x equals the number of routing device and Ethernet jack setups per room.

Design Approaches:

There are various methods that can be used to implement IP Address sharing. One of them is accomplished with the use of a special server running NAT software (a proxy server). Essentially, routing is done via software that is installed in a server. Hence, the NIC (Network Interface Card) on the server attached to the hub would receive a URL. The NIC would pass the URL to the proxy software where the address of the client would be recorded for proper data routing. This method, however, is expensive and wears down the server as it uses a lot of system resources. In addition, it is the least feasible because

one needs to purchase, and setup, a server at every RJ45 jack, connect a hub to each server, and install proxy software to run NAT. Such a setup would require extensive building modifications to secure the equipment from the general public.

The next, more feasible but still expensive, method requires the use of an operating system with built-in NAT software. Such an operating system is readily available on the Internet (any Linux distribution) or can be purchased (Red Hat Linux). This setup, though, still requires a hub and a server but at least does not require the purchase of special proxy software. In addition, because of the fact that it is a Linux system, it is more secure and stable than other Windows systems. As mentioned above, this method would also require extensive building modifications, as one would still need to secure large pieces of computer equipment.

Finally, the last method that can be applied requires the use of a router/switch and hub. This is the most feasible, least expensive way to provide IP Address sharing. The only thing required to accomplish this is a router/switch (such as a LINKSYS Cable/DSL Router), which is much less expensive than setting up a server, and a hub. The router is configured and left in charge of assigning dynamic IP addresses to its users, routing IP packets to the correct nodes, and keeping a fast, reliable, and secure link to the Stevens servers. Little or no building modifications would be required with this implementation. All three of these methods will be considered based on ease of implementation, ease of use, reliability, speed and efficiency, cost, and ease of maintenance. Of these criteria, the most emphasis will be place on cost and ease of implementation followed by reliability, speed, and maintenance and ease of use in order of importance.

Watermarking has two main categories: perceivable and non-perceivable. We want to explore the invisible watermarks, and it is assumed that when the term watermark is used alone it is referring to a non-perceivable watermark.

Using a perceivable, or visible, watermark means marking the data so that it is easy to "perceive" that the data is copyrighted and who owns the data. Visible watermarks are not necessarily considered as a reliable method of copyright protection simply because it is to easy task to remove the watermark, thereby also removing any claim of rightful ownership.

On the other hand, non-perceivable, or invisible, watermarks cannot be detected by inspection of the data. There are two basic methods for inserting watermarks: Spatial domain, and the Transform domain.

Since data is normally stored as a byte, Spatial domain watermarking techniques modify selected data points by adding a constant. The maximum magnitude of the constant is normally selected based on qualitative measures. Basically, the magnitude of the constant is increased until just before it can be perceived. After this value has been obtained then other methods, not to be discussed at this time, are used to select the magnitude of the constant.

The second method used, watermarking in the Transform domain, takes the data and transforms it to a different domain, watermarks the data, then transforms back to the Spatial domain. There are many different kinds of transforms. To name a few: Fourier Transform (FT), Discrete Cosine Transform (DCT), and Wavelet Transforms. The transform that is most often used with watermarking is the DCT.

The method that will be implemented in our senior design project will be based on the research paper by Cox, "Secure spread spectrum watermarking for images, audio, and video" [1]. The following steps explain how to insert a watermark using Cox's algorithm:

1. Separate the audio file into blocks or segments, the sizes that are normally used are 8, 16, and 32.
2. Take the DCT of each block.
3. Insert the watermark into the DCT coefficients in descending order of magnitude, ignoring the DC coefficient.
4. Take the inverse DCT of the marked data.

Extraction of the watermark is accomplished in the following manner:

1. Separate both the marked and original data into segments. The segment size must be the same size that was used during insertion.
2. Take the DCT of each block for the marked and unmarked data.
3. Using the original data and ignoring the DC coefficient find the coefficients in descending order of magnitude. At each location subtract the coefficient of the original data from the watermarked data, the result will be the watermark.

It should be noted that we have programmed all the procedures in a special toolbox in Matlab which will carry out this simulation process. The toolbox will actually apply the DCT principles in the fashion describe in Cox research paper.

Financial Budget:

In the design of this project we are looking at cost of testing and mostly man-hours that will be spent in the design stages. Research which will be conducted including reading the reference papers in the advance study by previous professionals. Time in telephone conference with Iowa State

University research student who conducted watermarking studies. Note the following items need for hardware and software design requirements.

1. Sony WDC-5000 High Sensitivity Cassette Recorder, for capturing of voice with two noise filters. This device will assist in the clean analog to digital playback when digitizing the audio files. Estimated Cost: \$399.99
2. JVC Camcorder VHS for capturing of video with noise filters. This device will assist in the best capture of analog source signal. In addition we need to have a tripod for mounting. Estimated Cost: \$575.00
3. Sony Video Hi-Fi Cassette Recorder Model SLV-M20HF. This device will be used for precision playback of video cassette (VHS) as analog source signal. Estimated Cost: \$499.99
4. Matrox Video Capture Card Model Marvel G400-TV Out. This device which will be configured in PC hardware is a 256 bit rendering card. It will allow you to capture at high frame rates of 30fps. At the same time it will accomplish all compression in the hardware environment. Estimated Cost: \$365.00
5. Media Cleaner Pro 4.02. This professional compression software will be used to do the compress and sampling of all digitized files. It is the defacto of all compression in the digital world, and used by most professionals. Estimated Cost: \$1500.00
6. Soundforge 4.5g. Clean up and manipulation of all audio and video data types. This is the device which will be used to actually look at the data and compare the Fourier Series and collect information. Estimated Cost: \$699.99
7. RAM, Processor Requirements. 512MB of memory will be needed to accomplish the successful compression of all media due to the amount of data to process. AMD 800MHz Athlon processor will be used as the CPU for the power of manipulation. Estimated Cost of Both: \$1000.00
8. Matlab 5.3 Professional Edition. This software will be used for apply the DCT technology in watermarking applications. Estimated Cost: \$499.99
9. Linksys Router BEF-4 Port: This is the device used for all IP sharing manipulation which acts as a firewall. It is a DHCP server which is a simulator device for the Stevens environment. Estimated Cost: \$180.00
10. Cabling and Wiring. Estimated Cost: \$120.00
11. Engineering team will perform research at 5 hours weekly for the next 8 weeks in fiscal year 2000. Additional research will be conducted in fiscal year 2001 at hours weekly for another 16 weeks. Rate of work \$150/hr. Man-hour Estimated Cost: \$18,000.000

Hardware and Software Budget: \$6264.96 - \$425.00

Engineering Team Payroll: \$18,000.00

Total Proposal Budget Requested: \$23789.96

Project Schedule:

Note the attachment of Project 2000, Gantt charts.

Conclusion:

This watermarking technique is very robust against most attacks, attacks being attempts to compromise ownership of the intellectual property. The most basic attacks are lossy compression (removal of information) and/or adding noise to the data.

The biggest weakness of this technique is that the original data is required to extract the watermark. This is a problem because this technique cannot be used in applications that need to identify the watermark. An example is a music player that only plays legal, copyrighted music. Basically this means you can identify the file but there is no way to use a client to identify the file as a security measure.

Students who miss their classes because of some on campus activities such as interviews, appointments, or other extracurricular activities can now listen and view to the lectures that they've missed during this time. This can be achieved by the similar concept that is now used outside of Student Service Center to view personal information. But, this would only allow one user at a time to use the computer. This is where we introduce our IP sharing concept into media streaming applications. This would allow upto 253 users to use the media streaming applications via a single computer which is already connected to Stevens high-speed fiber-optic network. It also has a built-in NAT technology which also acts as a firewall protecting your internal network. Now, since all the incoming students have laptops with a network card, all they have to do is just connect it to the Linksys box, and they can start viewing the lectures. This can further be used for other applications such as high-speed internal data sharing computer. This concept is far better than having 253 RJ_45 ports built into the wall. This is a new breakthrough in the media streaming and IP sharing technology.

References:

- [1] J. Cox, J. Kilian, T. Leighton, and T. Shamoan, "Secure spread spectrum watermarking for images, audio, and video," in IEEE Int. Conf. Image Processing, vol. 3, pp. 243-246, 1996.
- [2] N. Nikolaidis, I. Pitas, "Robust image watermarking in the spatial domain," Signal Processing vol. 66 no. 3, pp. 385-403, May 1998.
- [3] G. Voyatzix, N. Nikolaidis, I. Pitas, "Digital Watermarking: an Overview," IX European Signal Processing Conference (EUSIPCO'98), vol. 1, pp. 9-12, September 1998.

- [4] N. Nikolaidis, I. Pitas, "Digital Image Watermarking: an Overview," IEEE transactions publication no. 0-7695-0253-9/99, 1999.
- [5] J. Mark Ettinger, "Steganalysis and Game Equilibria," David Aucsmith (Ed.), Information Hiding 1998, LNCS 1525, pp. 319-328, 1998.
- [6] The background image was found at <http://www.samnet.net/david2014/Music.htm> on April 09, 2000 at 1:30 pm.
- [7] Information on Discrete Cosine Transform was found at: http://ikpe1101.ikp.kfa-juelich.de/briefbook_data_analysis/node61.html on April 25, 2000 at 9:16 am.†
- [8] More information on Discrete Cosine Transform was found at: http://www.zenith.com/mpeg_tutorial/DCxfrm.HTM on April 25, 2000 at 9:16 am.
- [9] Even more information on Discrete Cosine Transform was found at: <http://www.ee.ubc.ca/home/comlab1/irenek/etc/www/techpaps/introip/manual06.html> on April 25, 2000 at 9:16 am.
- Links to other sites
- <http://www.crcg.edu/projects/agent.html>
- <http://www.digimarc.com/>
- <http://207.25.71.25/TECH/computing/9901/27/mp3.idg/index.html>
- http://lci.die.unifi.it/~piva/Watermarking/watermark_audio.html
- <http://www.webreference.com/content/watermarks/>
- http://www.pcwebopaedia.com/Multimedia/digital_watermark.html

Appendices:

There are some additional software applications that we are planning to use in our design stage including sampling and ripping applications. Most of them are low level and will be used to experiment mostly. Due to the environment of networking we will have to purchase additional network cards, and network cabling. Most of these items will be purchased locally as the needs presents itself. For the most part this report should entail the major factors in the design and research areas.