International Journal of Engineering Research and Development
e-ISSN: 2278-067X, **p**-ISSN: 2278-800X, www.ijerd.com
Volume 6, Issue 3 (March 2013), PP. 23-27

Dual Mode Mpeg Steganography Scheme For Mobile and Fixed Devices

V.Saravanan[1], Dr.A.Sumathi[2], S.Shanthana[3], M.Rizvana[4]
[1,4]Assistant Professor, Department of IT, P.S.V. College of Engineering & Technology, Krishnagiri.
[2]Dr.A.Sumathi, Professor and Head, ECE Department, Adhiyamaan College of Engineering, Hosur.
[3]Lecturer, Department of IT, P.S.V. College of Engineering & Technology, Krishnagiri.

Abstract:- This paper reduces the detectable distortion in a Moving Picture Experts Group (MPEG) file during data hiding process, by introducing new bit embedding scheme. The new bit embedding scheme considers three factors, i.e., the n^{th} significant bit of each pixel, number of 1s or 0s in the pixel and block size. The MPEG frames are split into number of blocks and each pixel in it will be examined to embed the secret information. Depends upon the n^{th} significant bits and bits in the secret information, the least significant bit of each pixel will be altered. This proposed method of information hiding will help to solve the security issues in computer networks. The proposed system works in dual mode and suitable for mobile devices with low computational power and resources. Also, it improves security and reduces the detectable distortion.

Keywords:- Steganography, Macroblock, NSB, LSB, Video, Secret Information

I. INTRODUCTION

Steganography is an art of hiding information in multimedia elements like image, video and animation …etc. Generally, all the multimedia elements are stored in the storage devices as binary values. The binary values can be altered to hide secret information. Altering few bits may not change originality of the multimedia elements in considerable amount, but if the changes are too high then, originality of the Multimedia elements will be spoiled. So to hide few kilo bytes of information we need few mega bytes of multimedia elements. Combining both Steganography and cryptography together will improve the security dramatically.
Generally video Steganography will embed secret information into the video content by considering every part of the video frames with equal importance. So the capacity of the steganography could be limited to maintain low visual distortion (VD).
The media with secret information is called stego media and without hidden information is called cover media [1]. Steganalysis is a process of extracting information from the stego media. Steganalysis is just opposite to Steganography.

A. **Basic Concept**

Any video is made up of frames and each frame is made up of pixels. Each pixel represents a colour value and depends upon the video the pixel size will be from 1 bit to 4 bytes. These pixels will be stored in the computer memory in binary form.

Let us consider a 10 second video with 25 frames per second and each frame contains 80000 pixels (400 X 200) with pixel size 8 bits for discussion. The pixel with 8 bit size can able to represent 256 different colours, range from 00000000 to 11111111. The total number of bits in the video content (That is Size) can be calculated as,

Size = VL X FR X FS X BR

Where, VL is the video length, FR is the frame rate, FS is the frame size and BR is bit rate. For the above said video, Length is 5 Seconds, frame Rate is 25, frame size is 80000 and bit rate is 8. So, the actual size of the video can be calculated as,

Size = 10 X 25 X 80000 X 8 = 160000000 Bits.

Normally for human eyes the colour 11110000* and 11110001* will look like similar, since the difference is too low. Which means that the change in least significant bit (*LSB) may not be noticed by human eyes. If we alter #11110000 as #01110000, then the colour of a pixel will change to another colour. That is the change in the most significant bit (#MSB), will change the colour dramatically. This can be easily notified by everyone and the originality of the image will be spoiled. So it is clear that the secret information has to be stored in the LSBs and not in MSBs of the cover media to reduce the detectable distortion.

Let as consider a situation [2] that a person "A" wants to send secret information to another person "B" and the secret information is "Tomorrow Meet Me in College". This information should not be known to a person "C" who is an expert in hacking. In this situation A has to take a cover video of size eight times greater than secret information and he has to convert the secret information into binary form and then he has to store the secret information in the LSBs of each pixel one by one. The resultant video (stego video) will be send to B via computer network. Now C will catch the packets using various hacking tools available in the market and he can construct the video send by A to B (This is possible as said in chapter 2). Now C can just see the video and he might think that there is no secret in their communication. This is how one can cheat the hackers using Steganography.

B. Performance of the Steganography

The performance of a Steganography can be measured by three factors. They are security, capacity and detectable distortion (DD). The security must be high, so that the active attacks and passive attacks should not be succeed in finding secret information. Security can be achieved by changing way of storing the bits. For example instead of storing first bit, second bit and third bit of secret information into LSB of first, second and third pixels respectively, it can be stored in second, fourth and sixth pixels respectively. By doing such variation in the bit alteration may confuse the steganalyst. The capacity of the steganography can be calculated as,

Capacity = (VS / BR) X NL

Where, VS is the Video Size, BR is the bit rate and NL is the number of LSBs altered to represent the secret information (This can be from 1 to 3, for low distortion 1 can be used).

So, capacity of the above said video can be calculated for 1 LSB alteration as,

Capacity = (80000000 / 8) X 1 = 10000000 Bits.

Similarly, for 2 LSBs alteration the capacity can be calculated as,

Capacity = (80000000 / 8) X 2 = 20000000 Bits.

Normally capacity of the Steganography [2] can be increased by altering more LSBs of a pixel. For example instead of changing only one LSB of a pixel, if we alter two LSBs then the capacity will become double. But increasing the capacity beyond certain level will create detectable distortion in the stego video. Without increasing the DD the capacity has to be increased. The DD of a Steganography must be low that is, the stego video should not have high visual artifacts (That is the change in the video content should not be notified easily by the humans).

In this paper, we are focusing more on Security and DD of the steganography process. The ability for human vision system to detect alterations in video sequences must be considered for proper bits embedding during steganograpy process. All above discussion is suitable and true for uncompressed video. It may not suitable for compressed video.

This paper is organized as follows. In section II, The security issues in computer networks are analyzed and the need for security mechanism is identified. In section III, basics about MPEG Video Encryption are discussed. In section IV, the proposed method of steganography is given. Finally conclusions are given in section V.

II. SECURITY ISSUES IN COMPUTER NETWORKS [2]

An easy way to comply with the paper formatting requirements is to use this document as a template and simply type your text into it. As discussed in [2], today everyone use computer networks and Internet to share resources and to exchange information between the connected nodes. This computer network can be classified into many types based on the properties like protocol, topology and architecture. Based upon the needed security level, cost factor, performance and implementation limits any one of this type can be used. Topology defines the physical arrangements of the nodes of a network. Widely known topologies are bus, ring, star, mesh and hybrid. In bus topology all the nodes will connected using a single cable (this cable will act as a backbone). Damaging the cable will cause network failure. The information can be easily hacked by hackers by taping the cable anywhere in the network. This is a simple and cheap topology to implement. In ring topology the nodes of a network will connect via a ring like cable. Comparing bus topology it is good in speed and information can be hacked easily by taping the cable.

In star topology the network devices like hub or switch will be used to connect all the nodes of a network. Tapping of single cable may not be useful to hack all the data of all the nodes if the network uses switches, because switch simply forwards the frame to a specific port, which is connected to specific node of the network. In case if a network uses hub, then taping a single cable is enough to monitor or hack the data of a network. Many hacking, network monitoring and packet capturing tools are available in the market. This will break the security in both wired and wireless networks. Mesh topology connects all the nodes of a network to each other. It is expensive because it needs more number of cables and network adapters. Here the advantage is

failure of single cable may not affect the network performance and the network will be more stable. During the information exchange the data will travel in multiple path, so hacking is tough than previous topologies.
Using architecture also we can classify the networks. Widely known architectures are peer-to peer and client-server. In peer-to-peer all nodes can communicate with each other without any specific server node to control. It is suitable for small companies or institutions where the number of nodes is less. Generally this type of architecture used to share resources like storage capacity, internet, printers, scanners and other things. Most of the small companies and DTP centres use this type of network for easy installation.
In client-server architecture a specific node can act as a NT Domain Controller, which controls all the nodes of a network. All the nodes can login to the server to get a specific service. During the login process the nodes has to send the user name, password and other information like text by captcha for proper authentication. The client-server architecture is good in case of security comparing peer-to-peer. Because of security reasons many big companies uses this type of architecture. Also, the security risk is very high in wireless networks than wired networks, since the signal spreads over air, the hackers can sit anywhere in the coverage area to hack the data.

Wireless Networks and Mobile Nodes

In wireless networks the communications happens with electromagnetic signals. These signals need no line of sight like infra red communication. This electromagnetic signal will spread in all the directions and any one can receive the signals by sitting anywhere in the network's coverage area. Thus we cannot able to provide physical security for the communication medium and providing security is tough in wireless network than wired network.
The nodes of the wireless networks are mobile in nature. The mobile node has many limitations comparing fixed nodes. They are
Low Computing Power
Low Memory
Limited Power Backup
Low Connectivity Speed
Because of the above mentioned limitations, the security algorithm or schemes developed for fixed nodes may not be suitable for the mobile nodes. Hence, a special care has to be taken while developing new algorithm or scheme related to security or other purpose.

III. MPEG VIDEO ENCRYPTION

Generally video compression techniques will reduce the redundancy in video data to reduce the size of the video file. Most video compression algorithms and codec uses both spatial image compression and temporal motion compensation techniques together. Also, most video codec uses audio compression techniques together to compress the audio streams. Generally the video compression algorithms use lossy compression because in lossless compression the video size could not reduce beyond certain range. The highly compressed video may present visible or distraction artifacts. Sequence of still images called frames may form a video data. Each frame is made up of number of pixels. Video compression typically operates on neighboring pixels, called macroblocks. These pixel groups or blocks of pixels are compared from one frame to the next frame. The sequence of frames contains both spatial and temporal redundancy that video compression algorithms try to make it in smaller size.

One of the most powerful techniques for compressing video is interframe compression. Interframe compression uses more than one frame in a sequence to compress the current frame, while intraframe compression uses only one frame and deals with number of pixels in it. The most commonly used method works by comparing each frame in the video with the previous or next one. If one frame contains areas, where nothing has changed comparing previous frame then, the system simply issues a short command to copy that part from the previous frame. If a group of frames have small changes comparing each other, then the system simply issues a command that tells the de-compressor to rotate, lighten, darken or shift the copy (This command is little longer than the previous case but shorter than the intraframe compression). The interframe technique is good in case the video is just played by the user, but when try to edit the video, problem will occur, because interframe compression makes the player to copy data from one frame to another, if the original frame is simply left, the following frames cannot be reconstructed properly during editing process.

Some video formats such as DV uses intraframe compression, making video editing easy. In the format like MPEG2 (That uses interframe compression), certain frames are there called "I-Frame", which may not allowed to copy data from other fames and requires more data than nearby fames. Rate control plays a vital role in high quality video encoding. Achieving the perceptual quality at a given bit rate through the proper bit allocation process is the main goal. Using the frame other frame types like P-Frame, B-Frame and D-Frame along with I-Frame, the Bit rate of the video can be adjusted as needed.

IV. PROPOSED SCHEME

The working principle of the proposed scheme is as shown in the figure 1. The source video has to be processed and the I-Frames have to be extracted. These I-Frames has to be split into fixed number of parts called macroblocks. For each macroblock N0 and N1 will be calculated as follows:

$$N0_{ij} = \sum_{k=0}^{bs-1} NSB0_{kl}$$

$$N1_{ij} = \sum_{k=0}^{bs-1} NSB1_{kl}$$

Where $N0_{ij}$ is the number of zero's in n^{th} significant bit (NSB, where MSB ≥ NSB ≠ LSB) of the pixel in macroblock (i,j) and $NSB0_{kl}$ can be calculated as follows

$$NSB0 = \begin{cases} 0 & if\ n^{th}\ Significant\ bit\ of\ the\ pixel\ (k,l) = 1 \\ 1 & otherwise \end{cases}$$

Similarly, the NSB1kl can be calculated as follows

$$NSB1 = \begin{cases} 0 & if\ n^{th}\ Significant\ bit\ of\ the\ pixel\ (k,l) = 0 \\ 1 & otherwise \end{cases}$$

Based on the condition N0 < N1 either 1s or 0s of every pixel has to be calculated as follows:

Case 1: If the condition N0 < N1 is true and If the number of 1s in the first pixel is odd and the first bit in the secret information is also 1, then no need to alter the LSB of the pixel. If the number of 1s in the first pixel is odd and the first bit in the secret information is zero then we need to alter the LSB of the pixel to maintain the number of 1s as even.

Case 2: If the condition N0 < N1 is false and if the number of 0s in a pixel is even and the respective bit in the secret information is 1 then, the LSB of the pixel has to be altered to make the number of 0s as odd. If the number of 0s in a pixel is even and the respective bit in the secret information is 0 then, no need to alter the LSB of the pixel.

Fig. 1: Proposed System Architecture.

Our proposed scheme has many advantages as listed below.

1. The LSB alone get altered. Hence the DD will be minimized.
2. LSB of few pixels alone will get altered and the probability for a pixel gets altered is 0.5.
3. Based on the condition (N0 < N1) the algorithm will behave differently. Hence, the attacker will get confused and security will get improved.

Dual Mode

The above said algorithm is good in security but poor in running time, since it takes more time in calculating N0 and N1. Hence it may not be suitable for the light weight mobile devices which have low processing power, battery backup and memory. To overcome this problem the proposed scheme works in two modes (Manual mode and automatic mode). In manual mode the key will be passed (optionally) contain information which reduces the running time by eliminating the calculation of N0 < N1. In both the mode the key has to be send to the destination through the secured channel (along with value for n (NSB), picture size, block size). In automatic mode the set of values generated by the condition N0 < N1 for each and every block has to be recorded and transmitted to the destination as a key for reducing the running time if the destination machine.

V. CONCLUSIONS

In this paper we have discussed in detail about the steganography, security issues in computer networks and MPEG encryption. We have proposed a new scheme of bit embedding which has many advantages. It improves the security and reduces the DD. But still it has to be improved further in the future to reduce the computational complexity and the current version is not suitable for very low configuration mobile devices with low connectivity and computing speed.

ACKNOWLEDGMENT

Our sincere thanks to our honourable Chairman **Dr.P.Selvam M.A., B.Ed., M.Phil., Ph.D., D.Litt.,** P.S.V. College of Engineering & Technology, Krishnagiri, for giving this opportunity. We express my profound gratefulness to our Principal **Dr.K.Rangasamy M.E., M.B.A., Ph.D.,** P.S.V. College of Engineering & Technology for his continuous encouragement in publishing technical papers.

REFERENCES

[1]. Y.-F.Ma and H.-J. Zhang, "A model of motion attention for video skimming," in Proceeding ICIP, VOL. 1, pp. 129 – 132, September 2002.

[2]. V.Saravanan and A.Neeraja, "Security Issues in Computer Networks and Stegnography", in Proceedings of 7th International Conference on Intelligent Systems and Control (ISCO 2013), pp. 363-366, Coimbatore, Tamilnadu, India, January 2013.

[3]. Z. Chen and K. N. Ngan, "Toward rate-distortion tradeoff in real-time color video coding," IEEE Transactions on Circuits and Systems for Video Technology, vol. 17, no. 2, pp. 158–167, Feb. 2007.

[4]. S. Battiato, G. Di Blasi, G. M. Farinella, and G. Gallo, "Digital mosaic framework: An overview," Eurograph. - Comput. Graph. Forum, vol. 26, no. 4, pp. 794–812, Dec. 2007.

[5]. S. Battiato, C. Guarnera, G. Di Blasi, G. Gallo, and G. Puglisi, M. Bubak, Ed. et al., "A novel artificial mosaic generation technique driven by local gradient analysis," in Proceedings of ICCS, Crakov, Poland, vol. 5102, pp. 76–85, Jun. 2008.

[6]. K. Solanki, U. Madhow, B. S. Manjunath, S. Chandrasekaran, and I. El-Khalil, "'Print and Scan' resilient data hiding in images," IEEE Transactions on Information Forensics and Security, vol. 1, no. 4, pp. 464–478, Dec. 2006.