Distribution of Multimedia Data using Steganographic Methods

Jackson Jose, Laljith Johnson,Vikas Maddala, Imran Mirza
Department of Computer Science
Mumbai University
Don Bosco Institute Of Technology
India
{jackfluence, laljith.johnson, maddala.vikas}@gmail.com, mirza@dbit.in

ABSTRACT: *Development of a multimedia website for direct multimedia data distribution between the creators (photographers or music bands or movie producers) and the end users (images for websites or companies or magazines or music for daily web-surfers or any company or advertisement). The multimedia data gets stamped with some recognizable feature using steganography and thus offers great potential for securing of data copyright and detection of infringers. This project report intends to give an overview of multimedia steganography, its uses and techniques. It also attempts to identify the requirements of a good steganography algorithm and briefly reflects on which steganographic techniques are more suitable for which applications.‘Palette-based image steganography using colour quantisation’,‘Bit manipulation’ are the various steganographic approaches for the multimedia data.*

Keywords: Video, Image and Audio Steganography, MPEG, JPEG

Received: 6 August 2012, Revised 28 September 2012, Accepted 2 October 2012

1. Introduction

One of the reasons that intruders can be successful is the most of the information they acquire from a system is in a form that they can read and comprehend. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is, through the use of steganography. Steganography is a technique of hiding information in digital media. In contrast to cryptography, it is not to keep others from knowing the hidden information but it is to keep others from thinking that the information even exists.

Steganography become more important as more people join the cyberspace revolution. Steganography is the art of concealing information in ways that prevents the detection of hidden messages. Steganography include an array of secret communication methods that hide the message from being seen or discovered.

Most of information is kept electronically. Consequently, the security of information has become a fundamental issue. Cryptography along with steganography can be employed to secure information. In this method, the message or encrypted message is embedded in a digital host before passing it through the network, thus the existence of the message is unknown. Besides hiding data for confidentiality, this approach of information hiding can be extended to copyright protection for digital media: audio, video and images which is the main aspect of our project.

The growing possibilities of modern communications need the special means of security especially on computer network. Thenetwork security is becoming more important as the number of data being exchanged on the internet increases. Therefore, the confidentiality and data integrity are requires to protect against unauthorized access and use. This has resulted in an explosive growth of the field in information hiding.

The main objective is to develop a website which shows how steganography can be utilized to distribute multimedia data over the internet by making author data as the steganographed content of the particular multimedia data. The website would provide an interface to input multimedia data which would include audio, video or image where the author has to provide his legal details so as to be steganographed within the multimedia data. The data is then displayed on the Website for distribution. In case there is an un-authorized distribution or piracy of the multimedia data the multimedia data can be checked for the presence of author information and thus legal action can be taken against any un-authorized user.

2. Proposed method for images

The main reason for using palette-based image representation is based on the observation that natural images usually use only a small percentage of the available RGB colour space. Quantization of colours can be done without severely degrading the image quality. Here mainly converting each image to BMP for simplicity and efficiency. Such palette based image formats usually limit the number of colours up to 256, keeping only a third of the colour image data. Although such limitation seems to be a cruel constrain, in most of the cases, this is still high enough for a decent approximation of the original full-colour image. The quantization is done only by grouping two similar colourentries in the palette into the same colour. For example, if we select two colours‘*a*’ and ‘*b*’ and find the closest colour by finding the difference between the squares of the two colours. We can then assign for instance binary choice 0 to ‘*a*’ and 1 to ‘*b*’ to represent the stego message. It is apparent that the distortion on the cover image is independent on the embedded data stream, since the distortion is introduced when assigning entry ‘*a*’ and ‘*b*’ with the quantized colour. Since they are almost identical, they can be used interchangeably, without affecting the outlook of the image.

2.1 The Embedding Procedure

For a palette-based image X with the colour map, a set of RGBAcolour P = {(r1, g, b1. a1),…., (rn, gn, bn, an)} and the embedding binary secret message M, such that | M |< | X |, (| . | denotes the length) equal to the length of the image. The embedding algorithm works as follows firstly initialize the colour table with all 256 colour entry numbers. With the particulars of size and bit depth specified. The colour is read in as intensity of red, blue and green pixels where A denotes the intensity level. Making use of appropriate data structure the colour values of the pixels are stored. It is easier to use a structrather than a class because reading and writingof all four colours at byte level can be done at once. The Java interface is created in order to collect relevant data from the user and to make it platform independent. Before the multimedia content is steganographed, encryption schemes like RSA, DES and AES are used along with a user password for security concern. The Encryption of data by using these methods ensures high level security of the steganographed data. For steganography 16 bit mask is used, after which row padding is done. Next step checks for any RLE compression. The bit space is accumulated by skipping the metadata wherever present by determining the red, blue and green shift. The steganographed image is built by comparing the old and the new bitmaps and replacing the colour with the closest colourby finding the difference between the squares of the two colours.

Algorithm for image uploading

```
1. Encrpyt the file
2. Form new encrypted file
3. Create password
4. Check whether image is in bmp
5. If not then go to step 6 else go to step7
6. Create temporary bmp file
7. Now hide the data
8. Verify given data
9. Convert images to bmp stegnographed file
```

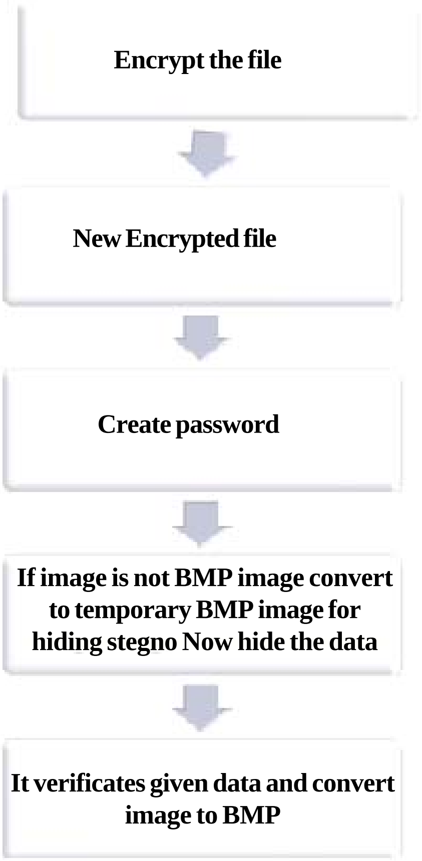
Encrypt the file
New Encrypted file
Create password
If image is not BMP image convert to temporary BMP image for hiding stegno Now hide the data
It verificates given data and convert image to BMP

Figure 1. Steps for encrypting and stegnographing image file

3. Proposed method for audio and video

Audio and Video Steganography are done using bit manipulation technique where a function named srand () generates a random sequence of numbers which is further used for embedding the data within its bit sequence. The function generates the random sequence of numbers in a sequential manner which is used for synchronisation and producing the same sequence of numbers for embedding and extracting the data from multimedia data. Here we also use strand function whose main objective is to return some random value. This random value is nothing but the value of the randompixels or the bits in video or image respectively. Srand function also guarantees the pixels or the value generated by it has as safe distance amongst themselves. These pixels or the bit position is actually used for steganagaraphy. At these particular position pointed by the function we can use stenographic methods like that of bit manipulation so that one can embed data in the cover file which can be audio or video. Secret file can be a simple message or any other media which is specified. Also the size of the secret message should not be larger than the cover file. A permissible limit is specified which actually is point of threshold and above which would result in degrading of the cover file. Thus we can define the maximum permissible limit of the secret file only after verifying the size of the cover file. This can ensure that the quality of the video or the audio is never degraded. Also after hiding and unhiding we can also get the pure flawless file as it is. Here we are developing the software which can hide and unhide the data in the cover file.

4. Procedure for Embedding Secret Message from Media

Using combined functionality of both the programming languages (c++ and java) the software gets divided into modules which make the work easier in fact simpler and efficient since the programming becomes user friendly and easier for usage and deployment.The embedding procedure starts withinputting the hidden file and checking for its extension and savingit.Using the java interface the source and destination addresses along with the message and password are fetched and passed on to a function which gets the size of the cover file and coverts it into BCD representation.The hidden message is first encrypted using encrypting technologies such as RSA, DES or AES. This follows conversion of the encrypted hidden message in character form to be embedded in the file, The function used here isembedChar (). Using a particular mask the hiddenmessage is embedded. After this step the password provided by the user is integrated with the message to make itsecure. A temporary file is created as a destination file to perform the steganography operation. The procedure includes copying 44 byte header + 54 bytes of extension space and also embedding verification bits as well as extension bits.The actual embedding starts in the temp file where function embedsize () which will define the size of the file and then embed the secret file after which the actual media data is embedded, in such a way that the quality of the file never gets reduced and safe insertion of secret message can be done. The user now can view his output steganographed file with the name steg. (extn) at the destination folder. The file can now be sent or uploaded anywhere and the authenticity of the file remains intact and only the author of the file can access it.

5. Procedure for Unhiding the Secret Message from Media

This procedure is analogous to the previous method as explained above. Here the user who wants to unhide the data from secret file will pass the parameters for unhiding it. All these parameters are captured by the java interface and is passed to various decrypting and extracting functions to actually unhide the data, next procedure is to read the file and check for its extension .The java interface collectsthe filename, destination filename and password which are required to locate and open the file. Various

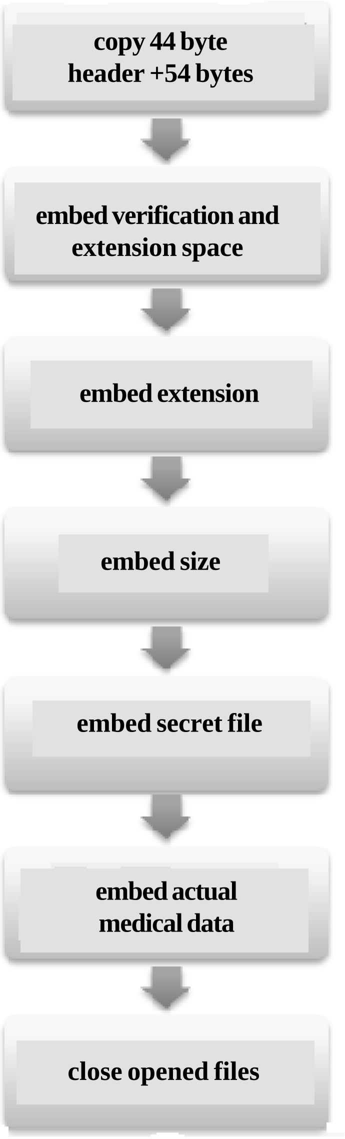
copy 44 byte header +54 bytes
embed verification and extension space
embed extension
embed size
embed secret file
embed actual medical data
close opened files

Figure 2. Steps for encrypting and stegnographing media file

error handling functions check for any errors and notify if required. This is followed by checking whether the object is message or a file. After checking, extract the size in BCD representation and then create an output file. The secret message is extracted and displayed to the user.

Algorithm for image uploading

1. Copy 44 byte header + 54 bytes
2. Embed verification and extension space
3. Embed extension
4. Embed size
5. Embed secret file
6. Embed actual media data
7. Close opened files

5. Developing a Web Interface

The web portal would include various modules which include data input, steganographing data within the multimedia data, easy distribution using the web portal, data given to authorized users. The web Interface would include a page to input the type of data and the respective details of the author is taken and then these details are steganographed with the original data and then displayed on the website for sale. All users can view the data but only authorized users can download it.If there is an illegal downloading or piracy of data then it could be checked on the website itself using the decrypting page which provides functions to check the identity of the author of the data by checking the steganographed content in the pirated data. Thus illegal use of the multimedia data can be minimized.

References

[1] Bin Liu, Fenlin Liu, Chunfang Yang, Yifeng Sun. (2008). Secure Steganography in Compressed Video Bitstreams,The Third International Conference on Availability, Reliability and Security.

[2] Andersen, R. J., P Petitcolas, F. A. On the limits of steganography. *IEEE Journal of Selected Areas in Communications*, Special Issue on Copyright and Privacy.

[3] Ko-Chin Chang, Chien-Ping Chang, Ping S. Huang, Te-Ming Tu. (2008). A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing, *Journal of Multimedia* , 3 (2), June.

[4] Hanafy, A., Gouda I. salama.,Yahya Z.Mohasseb. (2008). A Secure Covert Communication model Based OnVideo Steganography, *In*: Proc of the Int. Conf. IEEE Military Communication.

[5] Bin Liu, Fenlin Liu, Chunfang Yang, Yifeng Sun. (2008). Secure Steganography in Compressed Video Bitstreams, *In*: Proc of the Int. Conf. IEEE ARS, p 520-525.

[6] Dai, Y. J., Zhang, L. H.,Yang, Y. X. (2003). A New Method of MPEG VideoWatermarkingTechnology. *International Conference on Communication Technology, In*: Proceedings (ICCT).

[7] Wu, D. -C., Tsai, W.-H. (2003). A steganographic method for images by pixel-value differencing, Pattern Recognition Letters, 24, p. 1613–1626.

[8] Langelaar, G. C., Lagendijk, R. L. (2001). Optimal Differential Energy Watermarking of DCT Encoded Images and Video. *IEEE Trans. on Image Processing*, 10 (1)148-158.

[9] Lee, Y. K., Chen, L. H. (2000). High capacity image steganographic model, *In*: IEE Proceedings on Vision, Image and Signal Processing, 147 (3) 288-294.

[10] Hartung, F., Girod, B. (1998). Watermarking of uncompressed and compressed video, *Signal Processing*, Special Issue on Copyright Protection and Access Control for Multimedia Services, 66 (3) 283-301.