Prof. D P Gaikwad, Trupti Jagdale, Swati Dhanokar, Abhijeet Moghe, Akash Pathak /
International Journal of Engineering Research and Applications (IJERA)
ISSN: 2248-9622 Vol. 1, Issue 2, pp.102-108
www.ijera.com

Hiding the Text and Image Message of Variable Size Using Encryption and Compression Algorithms in Video Steganography

Prof. D P Gaikwad[1], Trupti Jagdale[2], Swati Dhanokar[3], Abhijeet Moghe[4], Akash Pathak[5]
(Department of Computer Science and Engineering
All India Shri Shivaji Memorial Society's College of Engineering, Pune
Maharashtra, India)

Abstract--- Steganography is a science that focuses on hiding specific messages using specialized techniques in such a way as only the sender and the intended receiver are able to disclose it. There are many different protocols and embedding techniques that enable us to hide data in a given object. However, all of the protocols and techniques must satisfy a number of requirements so that steganography can be applied. The secrete message can be hidden in text or video file. The main problem of existing steganography is that it should be assumed that the information to be hided is relatively short compared to the cover file. In this paper we have presented the steganographic technique for hiding the variable sized secrete messages into video file. We have used encryption and compression techniques. The compression is used when the secrete file is large before hiding it using LSB steganography technique. The password is used as secrete for encryption and decryption purpose. We can hide both text and image file different sizes into video cover file. We have used the authentication for login and logout the system for making system more secure and robust. The only authorized user can hide and disclose the message. The text and image file of different sizes are used to test the system. We found that the system satisfy all requirements of steganography. The system is secured and more robust.

Keywords—Encryption, Compression, Authentication, LBS method, Password, LZW, AES.

1. INTRODUCTION

Steganography is the art of hiding information that prevents the detection of hidden messages. *Steganography*, derived from Greek, literally means "covered writing." There are many methods include invisible inks, microdots, character arrangement, digital signatures, covert channels, and spread spectrum communications[11]. In history, Ancient Greeks wrote text on wax covered tablets to hide the message. Another ingenious method was to shave the head of a messenger and tattoo a message or image on the messenger's head. After the hair grew back, the message would be undetected until the head was shaved again. In electronic era, the motivation of hiding secrete message in different multimedia and secure communication via Internet is increased. Steganography is one of the most popular ways for secret communication. In steganography secrete message can be hidden in voice, video, text and image [1]. There are many to embed information into a popular media using steganography. A good example of this is the relationship between a recoded song, and its lyrics. The audio file containing the recording is much larger than the song lyrics stored as a plain ASCII files. Therefore it is probably safe to assume that the smaller file could be steganographically embedded into the larger one without impacting the quality. Important domains, besides classic computing, where steganography can be applied are domains using mobile and embedded devices especially mobile phones. In this project we state the fact that steganography can be successfully implemented and used into a next generation of computing technology with image and video processing abilities. This project concentrates on the Video Frame dynamics in order to create a steganographically driven Video file. The LSB method used for this project which satisfies the requirement of steganogaphy protocols. This research will include implementation of steganographic algorithm for encoding data inside video files, as well as technique to dynamically extract that data as original

2. BASIC CONCEPT OF STEGANOGRAPHY

2.1 Requirement of Steganography

There are many different protocols and embedding techniques that enable us to hide data in a given object. However, all of the protocols and techniques must satisfy a number of requirements so that steganography can be applied correctly .The following is a list of requirements that steganography techniques must satisfy [15][5].

1. The integrity of hidden information after it has been embedded inside the Stego object must be correct. The secret message must not be changed in any way such as additional information being added, loss of information or changes to the information after it has been hidden. If secret information is changed during steganography, it would defeat the whole point of process.
2. The stego object must remain unchanged or almost unchanged to the naked eye. If the stego object changes significantly and can be noticed, a third party may see that information is being hidden and therefore could attempt to extract or destroy it.
3.In steganography. Changes in the stego object must have no effect on the message. Imagine if you had an illegal copy of an image that you would like to manipulate in various ways. These manipulations can be simple processes such as resizing, trimming or rotating the image. The Stegano inside the image must survive these manipulations.
4. Otherwise the attackers can be very easily removing the Stegano and point of steganography will be broken.
5. Finally, we always assume that the attacker knows that there is hidden information inside the steno object.

2.2 Basic Techniques of Steganography

There are many techniques for hiding information or messages in images. Common approaches are including.

(I) Least significant bit insertion (LSB)
(II) Masking and filtering
(III) Transform techniques

Least significant bits (LSB) insertion is a simple approach to embedding information in image file. The simplest steganographic techniques embed the bits of the message directly into least significant bit plane of the *cover-image* in a deterministic sequence. Modulating the least significant bit does not result in human-perceptible difference because the amplitude of the change is small.
Masking and filtering techniques, usually restricted to 24 bits and gray scale images, hide information by masking an image, in a manner similar to paper watermarks. The techniques performs analysis of the image, thus embed the information in significant areas so that the hidden message is more integral to the cover image than just hiding it in the noise level.
Transform techniques embed the message by modulating coefficients in a transform domain, such as the Discrete Cosine Transform (DCT) used in JPEG compression, Discrete Fourier Transform, or Wavelet Transform. These methods hide messages in significant areas of the cover-image, which make them more robust to attack. Transformations can be applied over the entire image, to block through out the image, or other variants[6][7].

2.3 Least significant bit insertion (LSB) in Video Steganography

There are different kinds of steganography used in communication channel. The Plaintext, Still imagery, Audio and Video, IP datagram media can used for digitally embedding message. Text can be hided in an image by replacing some bites of the image according to the characters of the text. Similarly an image can be hided in another image by replacing bits of pixels of second image (In which we are hiding first image) corresponding to the pixels of first image matrix. Some commonly used techniques [9] [10] are:

- F 5 Algorithm
- LSB Coding
- Palettes Modification.

Here LSB coding is described in short**.** The pixel information of the source image is hided in the destination video frames such that each row of pixel is hided in first rows of multiple frames of the target. The process of hiding image into video frames is discussed here as. If we want to hide this image segment which is given as

(I) = 11100111 11101010
11011110 01101010

11011110 these 8 bits will be hided in 8 pixel of a video frame in following manner. Consider the eight pixels of a video frame as below.

(v) =10101001 10101001 10101001 10101001 10101001 10101001 10101001 10101001 After LSB replacement the above pixels will look like-
10101001 10101001 10101000 10101001 10101001 10101001 10101001 10101001 When all the columns of a frame are utilized next frame is selected. Next row of the image is hided in next row of the frames. The reverse process is used to get the secrete image message.

3. LITERATURE SURVEY

For studying the concepts of video steganography, we have surveyed many latest papers. In this section we have described the relevant papers of different authors. We thank these authors for providing the knowledge of video steganography. These paper were very important to us for studying the basic concept.

Arup Kumar Bhaumik, Minkyu Choi, Rosslin J.Robles, and Maricel O.Balitanas[2], the main requirements of any data hiding system are security, capacity and robustness It is very difficult to archive all these factors together because these are inversely proportional to each other. Authors have focuses on maximizing security and capacity factor of data hiding. The data hiding method uses high resolution digital video as a cover signal. It provides the ability to hide a significant quality of information making it different from typical data hiding mechanisms. They have used the large payloads like video in video and picture in video as a cover image.

Ahmed Ch. Shakir [1], the confidential communications over public networks can be done using digital media like text, images, audio and video on the internet. Simply hiding the contents of a message using cryptography was not adequate. Hiding of message should provide an additional layer of security. To provide the more security the author suggested the new procedures in steganography for hiding ciphered Information inside a digital color bitmap image. He has used quadratic method depending on the locations concluded by the binary image, beside of public key cryptography. He had concluded that the conjunction between cryptography and steganography produce immune information.

Andreas Westfeld and Gritta Wolf [3], in this work author have described a steganographic system which embeds secret messages into a video stream. Normally the compression methods are used in video conferences for securing acceptable quality. But usually, compression methods are lossy because reconstructed image may not be identical with the original. There are some drawback of compression and data embedding method. Signal noise and irrelevance are common examples of data embedding. But compression methods try to remove signal noise and irrelevance. If signal is compressed more, then there are fewer possibilities of data embedding. The author have solved this problem, they have investigated a typical signal path for data embedding. In this algorithm security is established by indeterminism within the signal path.

Sherly A P and Amritha P P [14], in this paper author have proposed a new compressed video Steganographic scheme. In this scheme the data is hided in compressed domain. The data are embedded in the macro blocks of I, P frames and in B frames. The novel embedding technique Tri-way Pixel Value Differencing (TPVD) is used to increase the capacity of the hidden secret information and for to providing an imperceptible stego-image for human vision. This algorithm can be applied on compressed videos without degradation in visual quality.

Saurabh Singh and Gaurav Agarwal [13], have presented a novel approach of hiding image in a video. In this approach, one LSB of each pixel is replaced by the one bit of secrete message. So It is very difficult to find that image is hidden in the video of 30 frames per second. The analysis is very difficult because each row of image pixels is hidden in multiple frames of the video. The intruder requires full video to unhide image. Authors have described the LSB algorithm in this paper. The proposed algorithm is very useful in sending sensitive information securely.

S.Suma Christal Mary [12], have proposed new Real time Compressed video secure Steganography (CVSS) algorithm using video bit stream. In this, embedding and detection operations are both executed entirely in the compressed. The proposed algorithm increases the security because the statistical invisibility of contiguous frames is used to adjust the embedding strategy and capacity.

4. PROPOSED WORK AND RESULTS

4. 1 Description of Proposed work

We have used the encryption technique before hiding the secrete message. Before encryption we can compression method if the secrete message is large. If the secrete message is small in size we don't need to compress the message. These two options are used which depends upon the size of message. We have used AES algorithm to encrypt the message. The LZW compression algorithm can be used if the compression is required. In the process of disclosing secrete message process, we have to login the system by giving the correct password. If the password is not correct as the password given at time of embedding, them the system will not allowed to disclose the secrete message. The LSB method is used to embed the message. Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover file. The algorithm of LSB method used in the system is described here as follows with the example as below.

For example, the letter A can be hidden in three pixels (assuming no compression). The original raster data for 3 pixels (9 bytes) may be

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

The binary value for A is **10000011**. Inserting the binary value for A in the three pixels would result in

(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)

To hide an image in the LSBs of each byte of a 24-bit image, you can store 3 bits in each pixel. A 1,024 ´ 768 image has the potential to hide a total of 2,359,296 bits (294,912 bytes) of information. If you compress the message to be hidden before you embed it, you can hide a large amount of information. To the human eye, the resulting stego-image will look identical to the cover image. The systematic flow diagram of the proposed system is shown in figure 1.

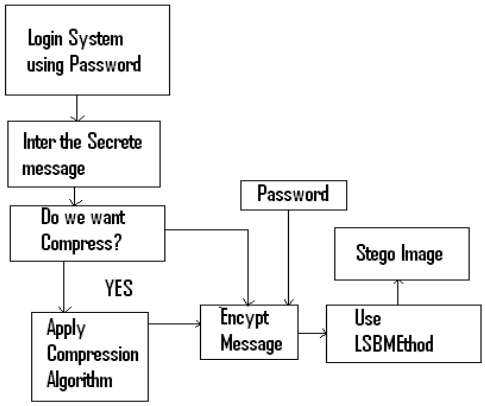

Figure 1. The Components of the System.

Unfortunately, it is vulnerable to even a slight image manipulation. Converting an image from a format like GIF or BMP, which reconstructs the original message exactly (lossless compression) to a JPEG, which does not (lossy compression), and then back could destroy the information hidden in the LSBs 24-bit images. The encryption algorithm which is used in system is described in short here. The Advanced Encryption Standard is encryption algorithm which has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits, Due to the fixed block size of 128 bits, AES operates on a 4×4 array of bytes, termed the *state matrix*. Most AES calculations are done in a special finite field. The following are the main steps of AES.

1) SubBytes — a non-linear substitution step where each byte is replaced with another according to a lookup table.

2) ShiftRows — a transposition step where each row of the state is shifted cyclically a certain number of steps.

3) MixColumns — a mixing operation which operates on the columns of the state, combining the four bytes in each column

4) AddRoundKey — each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule.

- Final Round (no MixColumns)

1) SubBytes

2) ShiftRows

3) AddRoundKey

For decryption the file we can use the same algorithm in inverse order. The AES Algorithm is used to encrypt the message before hiding. If the secrete text or image is large, we can compress it before the hiding. The compression is optional. For the compression, the LZW algorithm is used in the system. The LZW compression algorithm in its simplest form is given as below. A quick examination of the algorithm shows that LZW is always trying to output codes for strings that are already known. And each time a new code is output, a new string is added to the string table [4].

Routine LZW_COMPRESS

```
STRING = get input character
WHILE there are still input characters DO
   CHARACTER = get input character
   IF STRING+CHARACTER is in the string
table then
      STRING = STRING character
   ELSE
      output the code for STRING
      add STRING+CHARACTER to the string
table
      STRING = CHARACTER
   END of IF
END of WHILE
output the code for STRING
```

4.2 Flow chart of System

Here we are considering the different states as the login, logout, application with embed, extract, compress/decompress and compare. With the corrected information about password with the username given by user, the authorized user gets the access. Once getting the granted access user can use the application or he may logout. While using the system we can embed or extract the message file. Also we can compare the carrier file

and the embedded file by using compare option.

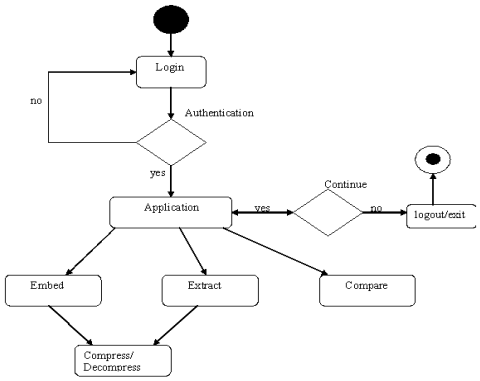

Figure 2. Flow Chart of the System

4.3 The results of Proposed work

When the system is executed the main menu is displayed for login process. Login is necessary for authentication purpose. The only authenticate user is allowed for using the system for both encryption decryption the message.

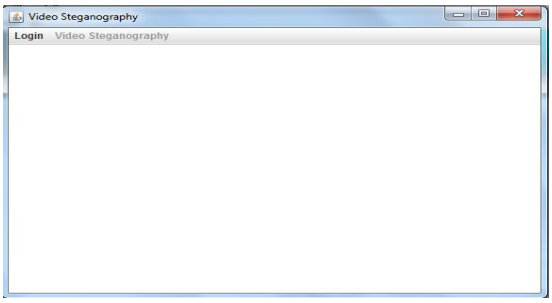

Figure 3. Snapshot of Main Menu

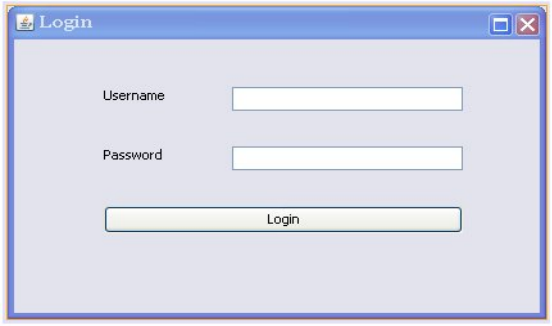

Figure 4 Snapshot of Login Window

After completion of login process, the User Selects the Carrier (Cover) File in which the message is to be hide. The user has to enter the name of output file. Then user can Selects the message file and enters a password to the message file. This password is used as the secrete key for encryption. When the button Embed is pressed we get the output file in directory.

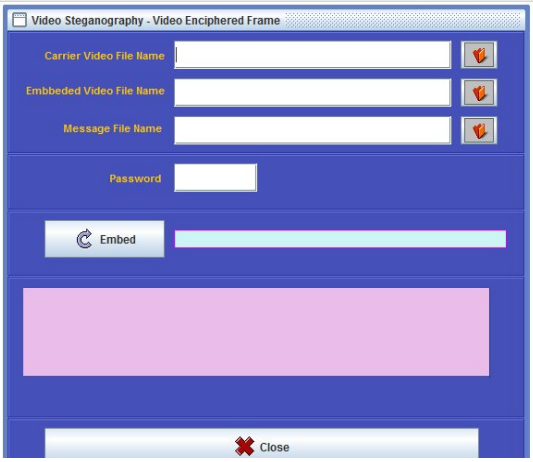

Figure 5. Snapshot of Embed Window

To extract the secrete message from Stego mage user has to give the name Stego file and password as secrete for decryption. Then we can get the secrete file in directory.

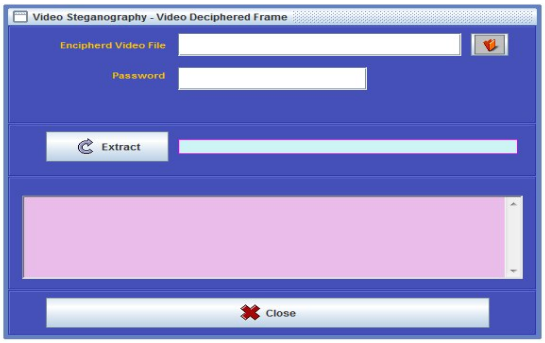

Figure 5. Snapshot of Extract Window

This allows user to compare the difference between the input file (original file) & the output file (encoded file).This only for the understanding of the User.

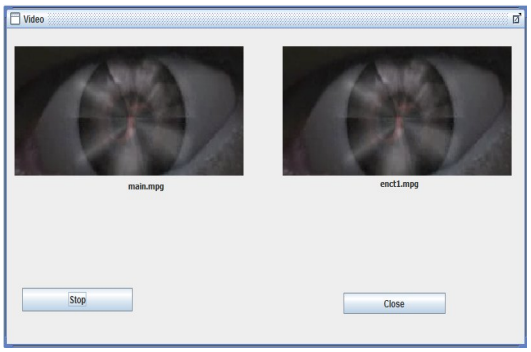

Figure 7. Snapshot to Display cover and Stego file for compare to file.

For completion of full product of Steganography, we have implemented the Email facility as well. We can send the Stego file to trusted user over network. The password and system should share among the Sender and trusted Receiver. Figure 8 allows the User to email the file as an attachment.

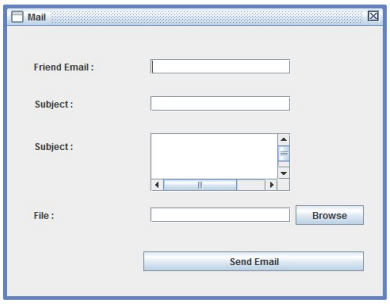

Figure 8. Snapshot of Window for Email the Stego File

5 CONCLUSION

In view of the great number of different embodiments to which the principles of our invention can be put, it should be recognized that the detailed embodiments are illustrative only and should not be taken as limiting the scope of my invention. Rather, we claim as my invention all such embodiments as may come within the scope and spirit of the claims, and equivalents there to.
So, Thus we Conclude that Steganography is a science that focuses on hiding specific messages using specialized techniques in such a way as only the sender and the intended receiver are able to decipher it, as well as knowing of its existence. Important domains, besides classic computing, where steganography can be applied are domains using mobile and embedded devices especially mobile phones. In this project we state the fact that steganography can be successfully implemented and used into a next generation of computing technology with image and video processing abilities.

FUTURE SCOPE

At present we are hiding the data in compressed video format, so in the future implementation of uncompressed formats may possible as well, so it may support MPEG4 format [16]. Multiple frames embedding are possible. Now we are embedding single frame at a time, but in future multiple frames embedding is also possible.

ACKNOWLEGDEMENT

We would like to express our gratitude towards a number of people whose support and consideration has been an invaluable asset during the course of this work.

REFERENCES

[1] Ahmed Ch. Shakir," Steno Encrypted Message in Any Language for Network Communication Using Quadratic Method", Journal of Computer Science 6 (3): 320-322, 2010 ISSN 1549-3636 © 2010 Science Publications.

[2] Arup Kumar Bhaumik, Minkyu Choi, Rosslin J.Robles, and Maricel O.Balitanas," Data Hiding in Video", International Journal of Database Theory and Application Vol. 2, No. 2, June 2009

[3] Andreas Westfeld and Gritta Wolf," Steganography in a Video Conferencing System", Information Hiding 1998, LNCS 1525, pp. 32-47, 1998. Springer-Verlag Berlin Heidelberg 1998.

[4] Cheng Cheok Yan, "Introduction On Text Compression Using Lempel, Zip, Welch (LZW) method",

[5] D.-C. Wu, and W.-H. Tsai.: A steganographic method for images by pixel-value differencing, Pattern Recognition Letters, Vol. 24, pp. 1613–1626, 2003.

[6] D. P. Gaikwad and Dr. S.J. Wagh, "Color Image Restoration for Effective Steganography", i-manager's Journal on Software Engineering, Vol. 4 l No. 3 l January - March 2010 65,pp.65-71

[7] D.P.Gaikwad and Dr. S.J.Wagh, "Image Restoration Based LSB Steganography for Color Image", AISA-PACIFIC Regional

Conference in ICTM-2010 on Innovations and Technology Management at Mumbai.

[8] Richard E. Woods & Rafael C. Gonzalez "Digital Image Processing", Book

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

[10] F 5 algorithm implementation: 2009, Fridrich, J.R.Du, M. Long: Steganalysis In Color Images, Binghamton, 2007.

[11] Neil F. Johnson and Sushil Jajodia," Exploring Steganography: Seeing the Unseen", George Mason University

[12] S. Suma Christal Mary, "Improved Protection In Video Steganopgraphy Used Compressed Video Bitstream ," International Journal on Computer Science and Engineering Vol. 02, No. 03, 2010, 764-766, ISSN: 0975-3397

[13] Saurabh Singh and Gaurav Agarwal,"Hiding image to video: A new approach of LSB replacement", International Journal of Engineering Science and Technology Vol. 2(12), 2010, 6999-7003

[14] Sherly A P and Amritha P P,"A Compressed Video Steganography using TPVD", International Journal of Database Management Systems(IJDMS) Vol.2, No.3, August 2010 DOI: 10.5121/ijdms.2010.2307 67

[15] Steganography on new generation of mobile phones with image and video processing abilities, as appeared Computational Cybernetics and Technical Informatics (ICCC-CONTI), 2010 International Joint Conference on 27-29 May 2010 in Timisoara, Romania ISBN: 978-1-4244-7432-5.

[16] Y. J. Dai., L. H. Zhang and Y. X. Yang.: A New Method of MPEG Video Steganographying Technology .International Conference on Communication Technology Proceedings (ICCT), 2003.