Creating an Image using Encrypted Sensitive word and Hide Over the Video Frame

[1]D. Priyadharshini, [2]M. Renuka Devi, [3]P. Palani kumar
[1]Nadar Saraswathi College of Engineering &Technology
[2,3]Karunya University

Abstract:-Creating An Image Using Encrypted Sensitive Words And Hiding over The Video Frame" is the software developed which uses the data hiding is one of the most better data and communication protection by hiding information into a media carrier technology called asstegnography . This method shows the way to create an image using encrypted sensitive text, hide over the video frame. In our daily life we are sending message through email, mobiles, social medias etc… But sometimes the unauthorized person (hackers) will easily hack our secret message. Now a days it's very difficult to send a secret message to sender to receiver . So this paper provide a high security for sending the secret message from sender to receiver. That is by creating an image using encrypted sensitive words and hide over the video frame. Mainly two methods are used in this "Cryptography, Stenography". This application mainly used in defense, business, etc… for sending secret message more securely.

I. INTRODUCTION

A. Need for Steganography in Video Files:

Currently, Internet, digital marketing, digital media and crypt techniques are getting more and more popular. So, the requirement of secure transmission of data also increased. Various good techniques are proposed and already taken into practice.Data Hiding is the process of secretly embedding the data in any multimedia file like image, video or audio form without changing it's quality. This apparent message is sent through the network to the recipient, where the actual message is separated from it. All these factors are inversely proportional to each other creating the so called data hiding dilemma. The focus of this paper aims at maximizing the first two factors of data hiding i.e. security and capacity coupled with alteration detection. This data-hiding method shows the high resolution digital video as a cover signal.

II. IMAGE USING ENCRYPTED SENSITIVE WORDS AND HIDING OVER THE VIDEO FRAME

Creating An Image Using Encrypted Sensitive Words And Hiding Over The Video Frame is based on encrypting the sensitive words over the video frames. It is very difficult for the hackers to find the particular frame over the video ,because 31frames are contently move over the video. This system is more user friendly and flexible. Data can be used in any form. More accurate result is produced .Fast and secure accesses to data are possible. To send the large amount of data, compression option can be used to deliver the message.
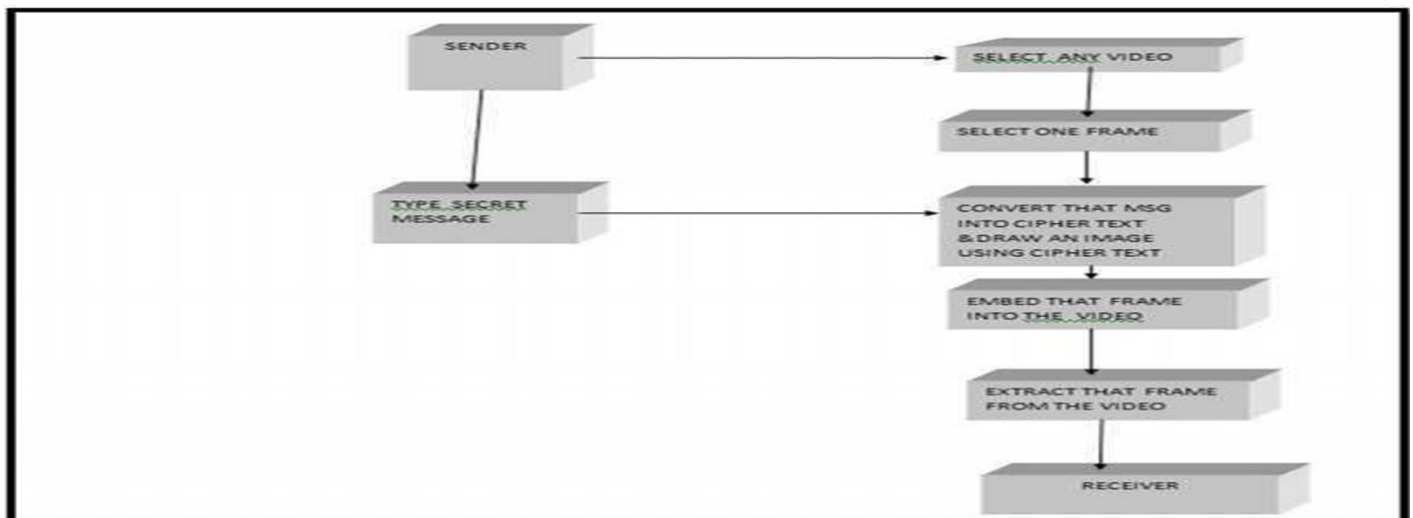

Figure1:System Architecture

III. IMPLEMENTATION AND RESULTS

A. Creating an Image and Message Hiding

A message, either encrypted or unencrypted, Then using pixel mapping method the system will draw a image using the encrypted sensitive words hidden in video file and transmitted over the Internet, a CD or DVD, or any other medium. This module is concerned with the hiding encrypted sensitive words over the video frame. Here we are converting the message or plain text in to cipher text format using RSA algorithm. Using RSA the message will be in the cipher text format with the help of key popular and secure public-key encryption methods. The encrypted words are can't understand the peoples very easily. The hidden cipher text message over the video frame.

B. Embedding

- The high resolution video is nothing but a sequence of high resolution image called frames. Initially I will like to stream the video and collect all the frames in bitmap format.
- Select any frame in that video.
- Type the secret message encrypt by using RSA algorithm
- Type the key.
- Create an image using encrypted sensitive words.(figure-1) By using pixel mapping method can draw the frame using text.
- Finally hide the frame into the same video.

C. Extraction

- It's the reverse process of the embedding.
- By using the decryption key the receiver extract the secret message from the video frame.This is an example of the image with sensitive Words(fig 2).This image is full of text message.. Initially the viewer reviewed, it as an image.
- The person will not recognize the words used to create this image.

Figure2:Image with Sensitive Words.

1.It is very difficult to recognize the text that hide in an image(fig 3).

2.This is an Innovative and efficient technology to find the secret message by creating an image.
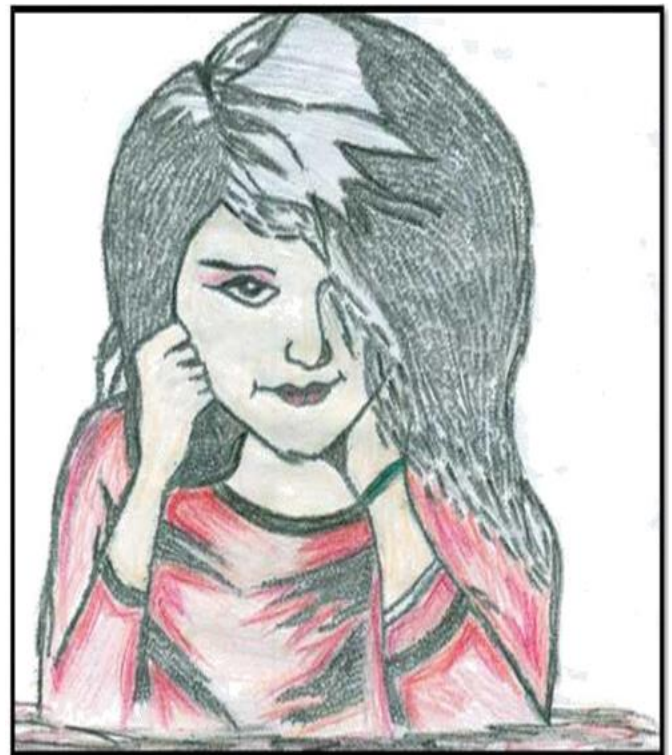

Figure 3:Image with Sensitive Words After Coloring

D. Data Size Estimation

Each frame of the Video is taken a data source for Data Hiding. First the maximum size of the hiding data is calculated . The size of the image is 2000 × 1000 and modified it to 2048 × 1024. On further calculations we get 786,432,000 chars that can be embed. We have followed the following equation mentioned below: ((Width × height) × 3 bits)/8 bits)/3 bytes × 3000 frames = char/video

And the image Bitmap size = 2048 × 1024 Step of calculations the maximum of hiding information:

- Each frame consist = 2048 × 1024 = 2, 097, 152 Pixels.
- Each pixel include 3 bytes (One byte we use single bit for encode data hiding) R = 1bit, G = 1 bit and B = 1 bit.
- Each frame = Pixels ×3 = 2, 097, 152 × 3 = 62, 915, 456 bits
- Each frame we can maximum hiding data is 62, 915, 456 bits/8 bits=786,432 bytes.
- If this video 3000 frames = 786, 432 × 3000 = 2, 359.296, 000 bytes (1 bytes=1 character) f. For 1 Character of Unicode we need 3 bytes/1 character of Unicode = 2,359.296,000 bytes/3 =786, 432, 000 chars.

E. Embedding the Image into the Video

Initially browse a video. While clicking the read option the information of particular video will be shown. Compression option is used because large amount of data to be extracted. Extract option used to convert into bit map format. Then by clicking the hide option new form will be opened. In that we have to browse a file to hide the text and key should be entered. In the other side either click the file name or enter the text which have to be hided. The encrypt button is used to convert the plain text to cipher text using RSA algorithm and click the hide button to hide the message. Finally click the save button to save the message. In RSA algorithm represent the message as an integer between 0 and (n-1). Large messages can be broken up into a number of frames. Each block would then be represented by an integer in the same range. Encrypt the message by raising it to the eth modulo n. The result is a cipher text message C.

F. Extracting The Message From The Video

By using the RSA algorithm, we can extract the secret message . This is to concerned with the decrypt the message from the hiding video frame. Here the cipher text words can be again convert into the plain text format. So, that the process will become much more secure.

IV.   CONCLUSION

A data hiding technique for high resolution video by hiding the encrypted text over the video. Our intension is to provide proper protection on data during transmission. For the accuracy of the corrects message output that extract from source we can use a tools for comparison and statistical analysis can be done. It is highly configurable, thus it may result in high data capacities to retrieve the original data. Finally, it can be easily extended, resulting in better robustness, better data security and higher embedding capacity.

REFERENCE

[1]. Data Hiding in Video Arup Kumar Bhaumik1, Minkyu Choi2, Rosslin J.Robles3, and Maricel O.Balitanas4 International Journal of Database Theory and ApplicationVol. 2, No. 2, June 2009.

[2]. Image Steganography and Steganalysis Using Pixel Mapping Method.International Journal of Engineering Research & Technology (IJERT)Vol. 2 Issue 11, November – 2013.

[3]. Johnson, N.F., Jajodia, S.: Exploring Steganography: Seeing the Unseen. Computer 31(2),26–34 (1998)CrossRefGoogleScholar

[4]. Artz, D.: Digital Steganography: Hiding Data within Data. In: IEEE Internet Computing,75–80 (2001)Google Scholar

[5]. Li, X., Wang, J.: A Steganographic Method based Upon JPEG and Particle Swarm Optimization Algorithm. Information Sciences 177(15), 3099–3109 (2007)CrossRefGoogleScholar

[6]. Chandramouli, R., Memon, N.D.: Analysis of LSB based image steganography techniques. In: IEEE International Conference on Image Processing, vol. 3, pp. 1019–1022 (2001)Google Scholar.

[7]. Kutter, M., Hartung, F.: Introduction to Watermarking Techniques in Information Techniques for Steganography and Digital Watermarking. In: Katzenbeisser, S.C. (ed.), pp. 97–119. Artec House (1999)Google Scholar

[8]. Mohamed, M., Al-Afari, F., Bamatraf, M.: Data Hiding by LSB Substitution Using Genetic Optimal Key-Permutation. International Arab Journal of e-Technology 2(1), 11–17 (2011)Google Scholar

[9]. Wang, R.Z., Lin, C.F., Lin, J.C.: Image Hiding by Optimal LSB Substitution and Genetic Algorithm. Pattern Recognition 34(3), 671–683 (2001)CrossRefMATHGoogleScholar

[10]. Chang, C.C., Hsiaob, J.Y., Chan, C.S.: Finding Optimal Least-Significant-bit Substitution in Image Hiding by Dynamic Programming Strategy. Pattern Recognition 36, 1583–1595 (2003)CrossRefGoogle Scholar