Video Steganography

Nikhil Wagh, Akanksha Gaikwad, Tejal Pawar, Vaishali Chothe

1.Information Technology&Sandip Polytechnic Nashik
2.Information Technology & Sandip Polytechnic Nashik
3.Information Technology & Sandip Polytechnic Nashik
4.Information Technology & Sandip Polytechnic Nashik

Abstract -Now a days with a development of internet technologies, this technology were highly used in current years. We can transfer the data through internet for data accurate and faster to the destination. Anyone can modify and misuse the data through hacking at the time. Steganography is an art of hiding the secret data and information inside the digitally covered information. the hidden message can be text, an image, an audio or video.

Steganography is a type of cryptography in which the secret message is hidden in digital information but in this project video steganography used for video which is transfer from sender to receiver It is used when number of images increasing, video processing issues 1and privacy safety. And most of the algorithm used for information hiding LSB algorithm, DCT algorithm, frequency domain analysis etc. but in this video we used LSB algorithm .

***Key Words*:**Steganography, LSB algorithm, DCT algorithm ,Video Steganography.

1. INTRODUCTION*(Size 11, Times New roman)*

When information is hidden inside video in program or person hiding the information will usually use the discrete cosine transform (DCT) method. DCT works by slightly changing the each of the images in the video, only so much though so it is not noticeable by the human eye. To be more precise about how DCT works, DCT alters values of certain parts of the images, it is usually rounds them up.

For example if part of an image has a value of 6.667 it will round up to 7. Steganography in videos is similar to that of steganography in images, apart from information is hidden in each frame of video. White space and tabs occur naturally in documents, so there is not really any possible way using method of steganography would cause someone to be suspicious.

1. Existing System

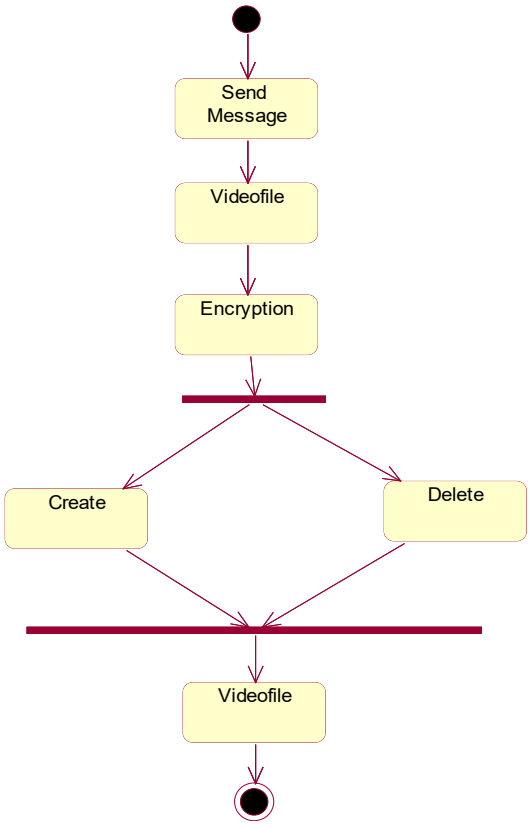
To protect important information we use cryptography. Steganography is different from cryptography, where the existence of the message itself is not disguised, but the content is obscured. Steganography could be considered as the dark cousin of cryptography. Cryptography assures privacy whereas Steganography assures secrecy. For e.g. Sending of encrypted credit card details over the internet is well known to a malicious user. But, the actual content is randomized or confused and hence not revealed. But, in Steganography the fact that the credit card details is being sent is kept secretly (as the message or the image appears innocent). The advantage of steganography over cryptography alone is that messages do not attract attention to themselves, to messengers, or to recipients. An unhidden coded message, no matter how unbreakable it is, will arouse suspicion and may in itself be incriminating, as in some countries encryption is illegal.

3. Proposed System

Encryption software protects internet connected computers from crackers and other online intruders. The technology is widely used to encrypt credit card

information, bank account numbers and other type of financial records so they can send safely and securely across the internet. Protect much of the intellectual content that's marketed on the web, such as music, Videos, articles, and software, restricting its availability to paying customers. This system helps to hide the information while sending the important and confidential documents in video files; it will be invisible for the third person.This system is helpful for the defense and security departments sending and receiving the confidential matters in emergency situations.

Encryption



DECRYPTION

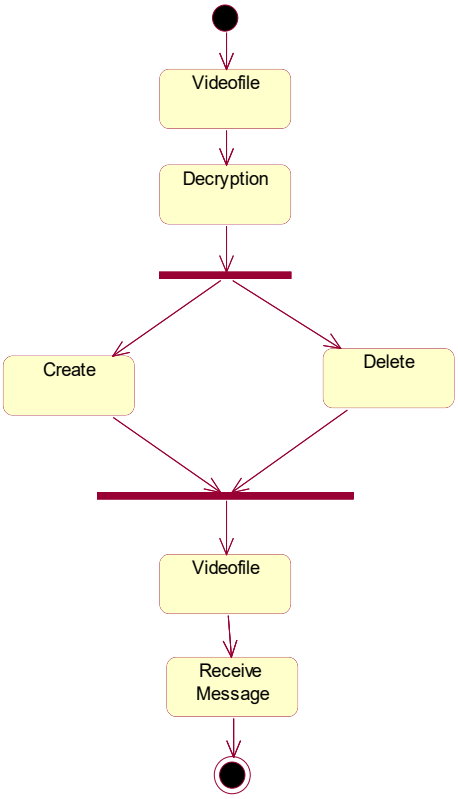


Table -1: Sample Table format

Take different video with varying the values of available samples

Sr.no.	Input video name	Size of extracted sound	Sample available	Resultant audio sound
1	Video1	24MB	154562	44.4MB
2	Video2	2MB	367828	111MB
3	Video3	213MB	47828	29.1MB
4	Video4	37MB	738293	14.9MB
5	Video5	56MB	71589	138MB

3. CONCLUSIONS

Steganography especially combined with cryptography, is a powerful tool which enables people to communicate without possible eavesdroppers even knowing there is a form of communication in the first place. These methods used in the science of steganography have advanced a lot over the past centuries, especially with the rise of computer era. Although the techniques are still not used very often, the possibilities are endless. Many different techniques exist and continue to be developed, while the ways of detecting hidden messages also advance quickly.

ACKNOWLEDGEMENT

We would like to thank our project guide **R.A.KAUTKAR** Assistant Professor for the guidance and help throughout the development of this project work by providing us with required information.

We would like to extend our heartiest thanks to our college for inspiring us to complete our project successfully. We convey our sincere thanks and gratitude to **Mr.V.J.Chaudhari, Head of the Department** for his valuable cooperation regarding the project.

An Endeavour over long period can also be successful by constant effort and encouragement. We wish to take this opportunity to express our deep gratitude to all the people who have extended their cooperation in various ways during our project work.It is our pleasure to acknowledge the help of all those respected individuals.

REFERENCES

1. Kesslet, Gary C. An Overview of Steganography for the Computer Forensics Examiner, Burlington, 2004.

2.Lin, Eugene and Edward Delp: A Review of Data Hiding In Digital Images, West Lafayette, 1999.

3. Hosmer, Chet. Discovering Hidden Evidence, Cortland, 2006.

4. Fridrich, J., R. Du, M. Long: Steganalysis Of LSB Encoding In Color Images, Binghamton, 2007