ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

Video Steganography Using Encrypted Payload for Communication

Sneha Bidkar[1], Priyanka Gaikwad[2], Shweta Chousalkar[3], Prajakta Avhad[4], Prof.Shikha Pachouly[5]

B.E. Student, Department of Computer Engineering, AISSMS COE, Pune, India[1-4]

Assistant Professor, Department of Computer Engineering, AISSMS COE, Pune, India[5]

ABSTRACT: Stegnography reveals the concept of hiding one media behind the other.It helps us to solve the security issues.The word stegno means covered and graph means writing,therefore it is used to write secret data on cover media.s Stegnography involves the texture synthesis process.Video stegnography involves texture synthesis that involves converting the video into no of frames and audio. This project involves reversible texture synthesis which resamples the smaller texture images into a larger local appearance image.However the task is still difficult it reveals the successful appearance of secret message.Stegnography is a vast concept and it includes vast no of medias.Stegnography uses the concept of cryptography,encryption and decryption.Stegnography is a vast concept.It allows us to keep the data at a secure level and introduces the concept of secret key.Secret key does not have a specific format.Thus stegnography provides data security and allows us to pass the secret message at a safely and accurately.

KEYWORDS: Cryptography, Encryption, Decryption , Secret Key

I. INTRODUCTION

Data security technology comes in many forms and protects data from a growing number of threats. Many of these threats come from external sources, but institutions must also focus on securing their data from within. Data protection methods include first data encryption which applies an icon to each data and does not grant access to encrypted data without a supported key. Second is data masking in which some data areas may be protected from the detection of external nuisance sources, as well as from internal personnel who may be using the data. For example, the first 12 digits of the credit card number can be hidden in a database. Third is data deleting that is sometimes data that is no longer active or used by all systems should be deleted. For example, if a customer requests that their name be removed from the mailing list, the data must be permanently deleted. And the last is flexibility which means backing up data, organizations can recover data if they are accidentally deleted, damaged, or stolen due to data breaches.

II. LITERATURE SURVEY

1. Exploring steganography: Seeing the unseen
AUTHORS: N. F. Johnson and S. Jajodia,
Steganography is the art of hiding information in ways that prevent the detection of hidden messages. It includes a vast array of secret communications methods that conceal the message's very existence. These methods include invisible inks, microdots, character arrangement, digital signatures, covert channels, and spread spectrum communications. Steganography and cryptography are cousins in the spy craft family: cryptography scrambles a message so it cannot be understood while steganography hides the message so it cannot be seen. In this article the authors discuss image files and how to hide information in them, and discuss results obtained from evaluating available steganography software.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

2. Hide and seek: an introduction to steganography,
AUTHORS: N. Provo's and P. Honeyman
Although people have hidden secrets in plain sight-now called steganography-throughout the ages, the recent growth in computational power and technology has propelled it to the forefront of today's security techniques. Essentially, the information-hiding process in a steganography system starts by identifying a cover medium's redundant bits (those that can be modified without destroying that medium's integrity). The embedding process creates a steganography medium by replacing these redundant bits with data from the hidden message.

3. Information hiding-a survey
AUTHORS: F. A. P. Petit colas, R. J. Anderson, and M. G. Kuhn,
Information-hiding techniques have recently become important in a number of application areas. Digital audio, video, and pictures are increasingly furnished with distinguishing but imperceptible marks, which may contain a hidden copyright notice or serial number or even help to prevent unauthorized copying directly. Military communications systems make increasing use of traffic security techniques which, rather than merely concealing the content of a message using encryption, seek to conceal its sender, its receiver, or its very existence. Similar techniques are used in some mobile phone systems and schemes proposed for digital elections. Criminals try to use whatever traffic security properties are provided intentionally or otherwise in the available communications systems, and police forces try to restrict their use.

4. A high-capacity steganography approach for 3D polygonal meshes,
AUTHORS: Y.-M. Cheng and C.-M. Wang,
We present a high-capacity steganography approach for three-dimensional (3D) polygonal meshes. We first use the representation information of a 3D model to embed messages. Our approach successfully combines both the spatial domain and the representation domain for steganography. In the spatial domain, every vertex of 3D polygonal mesh can be represented by at least three bits using a modified multi-level embeds procedure (MMLEP). In the representation domain, the representation order of vertices and polygons and even the topology information of polygons can be represented with an average of six bits per vertex using the proposed representation rearrangement procedure (RRP).

III. RELATED WORK

Most picture steganography calculations embrace a current picture as a spread medium. The cost of inserting mystery messages into this spread picture is the picture mutilation experienced in the stego picture. This prompts two disadvantages. In the first place, subsequent to the measure of the spread picture is settled, the more mystery messages which are installed take into consideration more picture twisting.Hence, a trade off must be come to between the implanting limit and the picture quality which brings about the constrained limit gave in any particular spread picture. Review that picture steganalysis is a methodology used to distinguish mystery messages covered up in the stego picture. A stego picture contains some bending, and paying little heed to how minute it is, this will meddle with the characteristic components of the spread picture.This prompts the second downside on the grounds that it is still conceivable that a picture steganalytic calculation can overcome the picture steganography and hence uncover that a concealed message is being passed on in a stego picture.

IV. APPLICATIONS

1. **Confidential information hiding:**It involves hidind confidential information for communication purpose
2. **Avoids data alteration:**It involves protecting the data and avoiding changes to it by any means.
3. **Access the control system for digital media:**It involves accessing the control over a particular system and avoiding any changes to the system.
4. **Media Database systems:**It involves storing the media in the database and providing protection to it.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

V. EXISTING SYSTEM

The multitude of methods and varitions have been used in data security model such as simply appling an encryption algorithm to data or authenticate using usernames and passwords. Many websites and software programsoften requires a password authenticated login. A strong password can be difficult to decipher and dramatically increase the time required to crack it. Use of encryption and other obfuscation techniques to hide data in relational databases, as well as data stored in the decoded computing architectures of big data platforms, to protect personal dataprivacy, achieve compliance, and reduce the impact of cyber attacks and accidental data leaks. The most recent work has focused on texture synthesis by example, in which a source texture image is re-sampled using either pixel-based or patch-based algorithms to produce a brand new synthesized texture image with similar local appearance and random size.

Disadvantages Of Existing System:

- To extract messages the output of the stego synthesized texture image is photographed before applying the data-detecting mechanism. The capacity provided by the method depends on the number of the dotted patterns. However, their methodology had a small error rate of the message extraction.
- Storing passwords on your computer can also pose a significant risk because they can be used to protect you from your various services and steal your identity if someone succeeds in taking control of your compute.

VI. PROPOSED SYSYTEM

Experimental results have confirmed that our proposed algorithm can offer different numbers of embedding options, produce visually plausible (imaginable) texture images and restore the source text. We proposed an image reversible data hiding algorithm which can recover the cover image without any distortion from the stego image after the hidden data have been extracted. First, we will define some basic nomenclature to be used in our algorithm. The first difference is that the shape of the overlapped space. We believe our proposed scheme offers substantial benefits and provides an opportunity to extend steganography applications.

The aim of the proposed system is to improve the security and speed of operation of crypto-stegosystem. So the system designed is a highly secured computerized crypto-steganographic tool based on three different stages which include Encryption ->Embedding -> Encoding. The proposed system is designed and built with reusability and stability in mind and also features a user friendly GUI (Graphical User Interface) interface that allows the user to encode/hide information into a carrier image. With this algorithm, the security of data can be improved and ensured as it is the encrypted text and not the plain text that is embedded in the image. Our proposed system provides use of more than one data security technologies i.e data encryption and data masking. Our system uses cryptography to first encrypt the data and then embed the encrypted data into a media file as data masking thus providing a dual protection mechanism for the the data.

Advantages of Proposed System

Our approach offers three distinct advantages.

1. Our scheme offers the embedding capacity that is proportional to the size of the stage texture image.
2. A pilarcryptography algorithm is not likely to defeat our steganography approach.
3.The reversible capability inherited from our scheme provides functionality which allows recovery of the source texture.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

VII. SYSTEM ARCHITECTURE

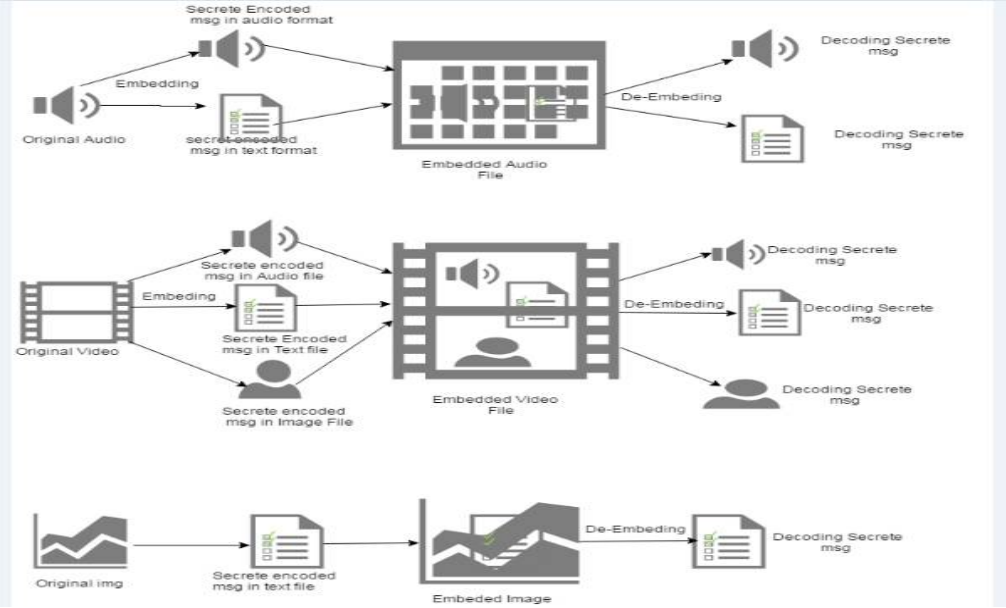


Fig.System Architecture

First of all the system starts and ask the user that is log in authority for Uploading message and video to access the system.After that sender select any cover media like video, audio or image. As per the above figure, we can select original video for hiding secret message. We enter text message which is the secret message and then with the help of secret key, we encrypt that message. When encryption is done, embeded video i.estego video will be generated at sender side. Sender send this stego video to the receiver. Reciever or authorized user will enter the same secret key which was used by sender. Reciever will decrypt that stego video and retrieve the secret message. Sender can hide images as secret message as well as audio as a secret message.

VIII. ALGORITHM

Blowfish algorithm:

Blowfish has a 64-bit block size and a variable key length from 32 bits up to 448 bits.[3] It is a 16-round Feistel cipher and uses large key-dependent S-boxes. In structure it resembles CAST-128, which uses fixed S-boxes.

The Feistel structure of Blowfish:

The adjacent diagram shows Blowfish's encryption routine. Each line represents 32 bits. There are five subkey-arrays: one 18-entry P-array (denoted as K in the diagram, to avoid confusion with the Plaintext) and four 256-entry S-boxes (S0, S1, S2 and S3).

Every round r consists of 4 actions:

Action 1:XOR the left half (L) of the data with the r th P-array entry

Action 2:Use the XORed data as input for Blowfish's F-function

Action 3:XOR the F-function's output with the right half (R) of the data

Action 4:Swap L and R

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

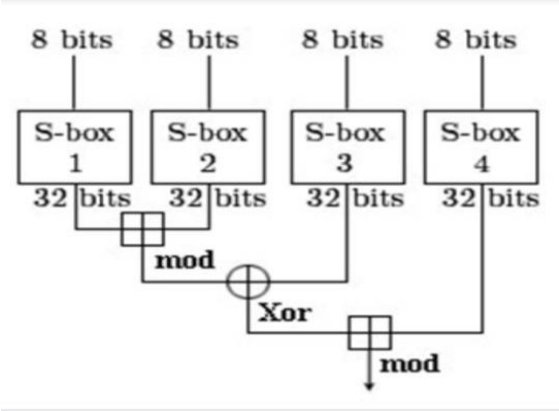
International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

The F-function splits the 32-bit input into four eight-bit quarters, and uses the quarters as input to the S-boxes. The S-boxes accept 8-bit input and produce 32-bit output. The outputs are added modulo 232 and XORed to produce the final 32-bit output (see image in the upper right corner). After the 16th round, undo the last swap, and XOR L with K18 and R with K17 (output whitening).Decryption is exactly the same as encryption, except that P1, P2, …, P18 are used in the reverse order. This is not so obvious because xor is commutative and associative. A common misconception is to use inverse order of encryption as decryption algorithm (i.e. first XORing P17 and P18 to the ciphertext block, then using the P-entries in reverse order).Blowfish's key schedule starts by initializing the P-array and S-boxes with values derived from the hexadecimal digits of pi, which contain no obvious pattern (see nothing up my sleeve number). The secret key is then, byte by byte, cycling the key if necessary, XORed with all the P-entries in order. A 64-bit all-zero block is then encrypted with the algorithm as it stands. The resultant ciphertext replaces P1 and P2. The same ciphertext is then encrypted again with the new subkeys, and the new ciphertext replaces P3 and P4.



IX. IMPLEMENTATION

In this system we are providing security using concept of crypto-steganography. User can hide any media like text,image ,audio and video behind video.Cryptography is used for encryption and decryption of data and steganography is used for hiding the data behind video.Firstly user do login into to system and after that user can browse media to hide and video from their system.

Following steps are used for implementing crypto-steganography on video:

- Login Module.

User can login into the system using username and password.If there is new user then he can register details using "register new user"buttonand after registering he can login to the system using username and password provided at the time of registration. After login successfully it directs to the mainclient page.

- Menu:

After logging to the system user will see the following page which contains options for choosing particular operation.User can hide the text,image,audio and video behind video.List of different operations is as follows:

1.Embed message:If sender want to hide text behind video then sender will choose this operation.
2.Embed file:If sender want to hide image ,audio or video behind video then sender will choose this operation.
3.Retrivemessage:If receiver want to retrieve text messege from video then receiver will choose this operation.

4.Retrive file :If receiver want to retrieve image,audio or video file from video then receiver will choose this operation.

- Sender Module:

After browsing all files from device now sender have to enter 8 digit secret key for encryption.If the secret key entered by sender is less than or greater than 8 digit then it will give an error message so the key should beof length 8

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

digit.Secret key is used for secure communication between sender and receiver.Sender also have to enter the secret data which he want to hide behind video i.e.data may be text,image,audio or video. In case of if the data is in the form of text the sender can write the text manually or he can also hoose a text file. Sender can also compress the videofile if he wants to reduce size.After entering all, the necessary details and clicking go button, actual encryption and embedding process is done and it will show message "Message Encrypted Successfully". This message means that the data to be hidden is successfully encrypted and embedded in the master file using cryptography and steganography algorithms.

- Retrieval Module:

After successfully sending the encrypted data to the receiver side, the retrieval process of the data starts at the receivers side. The retrieval process of the data contains de-embedding and decryption operation. First the receiver chooses the output file for retrieval process then it asks for the key to begin the retrieval process.After entering the key and on clicking "Retrieve now" first it will compare the secret keys entered by the sender and the receiver, if the two keys are equal then and only then the retrieval process starts. If the secret key entered by receiver is not same as secret key entered by sender then decryption will not start and it will show errormessageIn the de-embedding process the output file(i.e final encrypted video) choosen by the receiver in the start, the encrypted data is retrieved from the video authenticated secret keyOnce the retrieval process is complete successfully receiver can access the secret data(text,image, video or audio)which was hidden by sender behind video.In this way the crypto-steganography is implemented on video.

X. CONCLUSION

In this paper, we propose a system that allows a user to encrypt a secret message and hide its content into a cover image file as well as extract and retrieve the original data. Also, cryptography (encryption), compression and steganography techniques were combined and successfully implemented in order to secure a successful crypto -steganographic system with different levels of security. This work, satisfies the aim that says steganography is an effective way to obscure data and hide sensitive information. This allows an individual to hide data inside other data with the hope that the transfer medium will be so obscure that no one would ever think to examine the contents of the file. In other words, this work has successfully demonstrated that cryptography and steganography are used effective at securely concealing secret, vital or sensitive messages or information in media files (image file) without altering the cover file noticeably. The outcome of this study is also significant in cyber security as users of the cyberspace can use this application to secure their information from hackers and related cyber criminals. As a final thought, we see vast possibilities for the use ofsteganography in industrial espionage in the act of getting information out of an organization without anyone being aware.

REFERENCES

[1] N. F. Johnson and S. Jodie, "Exploring steganography: Seeing the unseen," Computer, vol. 31, no. 2, pp. 26-34, 1998.
[2] N. Provo's and P. Honeyman, "Hide and seek: an introduction to steganography," Security & Privacy, IEEE, vol. 1, no. 3, pp. 32-44, 2003.
[3] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding-a survey," Proceedings of the IEEE, vol. 87, no. 7, pp. 1062-1078, 1999.
[4] Y.-M. Cheng and C.-M. Wang, "A high-capacity steganographic approach for 3D polygonal meshes," The Visual Computer, vol. 22, no. 9, pp. 845-855, 2006.
[5] S.-C. Liu and W.-H.Tsai, "Line-based cubism-like image—A new type of art image and its application to lossless data hiding," IEEE Trans. Inf.Forensics Security, vol. 7, no. 5, pp. 1448-1458, 2012.
[6] I.-C. Dragoi and D. Coltuc, "Local-prediction-based difference expansion reversible watermarking," IEEE Trans. Image Process., vol. 23, no. 4, pp. 1779-1790, 2014.
[7] J. Fridrich, M. Goljan, and R. Du, "Detecting LSB steganography in color and gray-scale images," MultiMedia, IEEE, vol. 8, no. 4, (Dragoi, 2014)pp. 22-28, 2001.
[8] Rivest, Ronald L. (1990), "Cryptography", In J. Van Leeuwen. Handbook of Theoretical Computer Science 1, Elsevier.
[9] Bellare, Mihir; Rogaway, Phillip (21 September 2005), "Introduction", Introduction to Modern Cryptography, p. 10.
[10] "Overview per country", Crypto Law Survey, February 2013.