INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 03, March 2024, pp: 811-816

A CONCEALED INFORMATION SHARING SYSTEM USING CONTENT ADDRESSED STORAGE SYSTEM TECHNIQUE (CSST)

Gopika S[1]

[1]Rathinam College of Arts and Science, Coimbatore, India.

DOI: https://www.doi.org/10.58257/IJPREMS33030

ABSTRACT

Video Steganography is the process of hiding some secret information inside a video. The addition of this information to the video is not recognizable by the human eye as the change of a pixel color is negligible. This project aims to provide an efficient and a secure method for video steganography. The proposed method creates an index for the secret information and the index is placed in a frame of the video itself. With the help of this index, the frames containing the secret information are located. Hence, during the extraction process, instead of analyzing the entire video, the frames containing the secret data are analyzed with the help of index at the receiving end. When steganographed by this method, the probability of finding the hidden information by an attacker is lesser when compared to the normal method of hiding information frame-by-frame in a sequential manner. It also reduces the computational time taken for the extraction process. Video files are generally a group of images and sounds, so most of the existing techniques on images and audio can be applied to video files too.

Keywords- video, information, method, secret, index, process, images, files, steganography, containing.

1. INTRODUCTION

In an era dominated by digital communication and an unprecedented volume of sensitive information exchange, the preservation of confidentiality has emerged as a critical challenge. The continuous evolution of communication technologies has necessitated the development of innovative strategies to safeguard information from unauthorized access. Cryptographic methods have conventionally served as the cornerstone for securing data, employing mathematical algorithms to encrypt and decrypt sensitive content. However, in an age where surveillance and cyber threats persistently advance, the need for covert communication solutions has become imperative.This thesis explores the fusion of cryptographic and steganographic principles to address the inherent limitations of conventional secure communication methods. Steganography, the art of concealing information within seemingly innocuous carriers, offers a clandestine alternative to encryption. In particular, the integration of a robust Binary Steganography technique, known as Content Storage System Technique (CSST), holds promise for enhancing the covert communication paradigm. CSST, characterized by its ability to withstand steganalysis attempts, provides a foundation for secure and surreptitious information exchange. The central focus of this research is the development of a Crypto Stego Secret Information Sharing System that amalgamates cryptographic strength with the concealment capabilities of CSST. This system aims to facilitate secure communication while maintaining a low risk of detection, ensuring the confidentiality of shared information in various digital communication channels.

2. EXISTING SYSTEM

Researchers have implemented various approaches for information and data security to achieve secret communication. Steganography is a method of hiding the secret messages into the carrier medium such as image, audio, video etc. steganography technique is generally classified into three main types namely.

1. Technique exploiting image format.
2. Method embedding in frequency domain.
3. Method in spatial domain

The implementation of steganography as a method for achieving secret communication is not without its challenges. Existing systems face issues related to the detection and countermeasures, where sophisticated detection techniques and counter-steganography methods continually challenge the effectiveness of steganographic approaches. Another challenge involves the trade-off between capacity and quality, as embedding a significant amount of data within a carrier medium must be balanced with maintaining the quality of the medium. Security concerns, such as key management, authentication, and integrity, are crucial aspects, and the usability and practicality of steganographic techniques also pose hurdles, requiring a balance between complexity and user-friendliness. Legal and ethical considerations add an additional layer of complexity, with regulatory compliance and the potential for misuse raising important questions. Moreover, the dynamic nature of media formats necessitates ongoing adaptation of steganographic methods to keep pace with evolving technologies. Addressing these challenges requires continuous

research and innovation to enhance the security, efficiency, and practicality of hidden communication systems.

The implementation of steganography as a method for achieving secret communication is not without its challenges. Existing systems face issues related to the detection and countermeasures, where sophisticated detection techniques and counter-steganography methods continually challenge the effectiveness of steganographic approaches. Another challenge involves the trade-off between capacity and quality, as embedding a significant amount of data within a carrier medium must be balanced with maintaining the quality of the medium. Security concerns, such as key management, authentication, and integrity, are crucial aspects, and the usability and practicality of steganographic techniques also pose hurdles, requiring a balance between complexity and user-friendliness. Legal and ethical considerations add an additional layer of complexity, with regulatory compliance and the potential for misuse raising important questions. Moreover, the dynamic nature of media formats necessitates ongoing adaptation of steganographic methods to keep pace with evolving technologies. Addressing these challenges requires continuous research and innovation to enhance the security, efficiency, and practicality of hidden communication systems. Historically, steganography has roots in ancient practices, dating back to techniques used by ancient civilizations for secret communication. With the advent of digital technology, steganography evolved to exploit the imperceptible manipulation of bits within multimedia files. From basic LSB (Least Significant Bit) methods to more advanced transformations, researchers have continually refined steganographic techniques to ensure both concealment and resistance against detection. Among the myriad steganographic techniques, Content Storage System Technique (CSST) has emerged as a robust approach, focusing on maintaining the integrity of the embedded data while resisting detection attempts. CSST techniques often involve the careful manipulation of specific bits in a binary representation, aiming to minimize the impact on the carrier file's statistical properties. The resilience of CSST against various steganalysis techniques makes it an attractive choice for ensuring secure and covert information exchange. The synergy of cryptographic algorithms with steganographic techniques has been explored to enhance the security of information exchange. The integration of cryptographic frameworks ensures the confidentiality and integrity of the data being shared, providing an additional layer of protection. Modern cryptographic algorithms, such as Advanced Encryption Standard (AES) and Rivest Cipher (RSA), contribute to the robustness of the overall system. Efficient key management is crucial for secure communication systems. The distribution and exchange of cryptographic keys play a pivotal role in ensuring the confidentiality of shared information. Various key management strategies, including public-key infrastructure (PKI) and key exchange protocols, have been proposed to facilitate secure communication between parties involved. Performance evaluation metrics for steganographic techniques encompass factors such as embedding capacity, visual and auditory imperceptibility, and resilience against steganalysis. Comparative studies highlight the strengths and weaknesses of different techniques, guiding the selection of an optimal approach for specific use cases. As the proposed Stego system integrates CSST, a comprehensive performance evaluation will be vital to assess its efficacy in balancing security and usability. The application of cryptographic steganography in real-world scenarios spans diverse domains, including military communication, healthcare data exchange, financial transactions, and personal communication. Ethical considerations, such as the potential misuse of covert communication techniques, underscore the importance of responsible research and development in this field.

3. PROPOSED SYSTEM

A. Video selection and frame extraction

Initially the user should select a video file in the AVI format. After the selection the video will be converted into set of frames using frame grabber technique. After the frame extraction the data will be embedded into the frames. Video compression uses modern coding techniques to reduce redundancy in video data. Video compression typically operates on square-shaped groups of neighboring pixels, often called macro blocks. These pixel groups or blocks of pixels are compared from one frame to the next and the video compression code sends only the differences within those blocks.

In areas of video with more motion, the compression must encode more data to keep up with the larger number of pixels that are changing. Generally, the motion field in video compression is assumed to be translational with horizontal component and vertical component and denoted in vector form by for the spatial variables in the underlying image. Such as three steps search, etc.

B. Encryption

Encryption is the conversion of data into a form, called a cipher text that cannot be easily understood by unauthorized people. Original message is hidden within a carrier such that the changes occurred in the carrier are not observable. The information about the private key is used to encrypt the text. The text message will be encrypted and embedded into the frames.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 03, March 2024, pp: 811-816

C. Content Address Storage

Content Addressed Storage (CAS) holds significant promise in the realm of steganography, a technique concerned with concealing secret information within non-secret carriers to ensure covert communication. In this context, CAS provides a robust framework for storing and retrieving concealed data with a constant address reference. By employing CAS in steganographic systems, each piece of hidden information can be uniquely addressed based on its content, rather than its location within the carrier medium. This approach enhances data integrity and retrieval efficiency, as the concealed information remains immutable and easily retrievable, regardless of the carrier's alterations. Moreover, the constant address storage capability of CAS ensures that the hidden data remains securely embedded within the carrier, even amidst various transformations or attacks. Thus, integrating CAS into steganographic techniques holds the potential to bolster the security and reliability of covert communication channels, offering enhanced resilience against unauthorized access and detection.

D. Data embedding module

The video steganography composed of two main phases namely extraction of video files and embedding of secret message, as the secret message is already encrypted using AES it can be easily embedded into carrier image randomly using CSST.

The extraction of video results in frames as video generally composed of still images frames from the file video is extracted. For making this file more robust against attack or identification stego file is again encrypted using the Advanced Encryption Standard. The stego file generated is then transmitted over the communication channel which remains intact as a result of this complex data hiding method.

E. Video conversion

In video compression, a motion vector is used for motion estimation process. It is used to represent a macro block in a picture. Authenticated person after taking the second process, can see the video in the application, in that video it can detect the motion vector. After seeing this, the member uses the key to see the message sent to the receiver.

F. Extraction of original data

Decryption is the process of converting encrypted data back into its original form, so it can be understood. When the user inputs the correct key that is used at the decryption process, this will extract the original message that is encrypted and embedded.

4. DESIGN PROCESS

A. Enhancing Data Security

The general theme behind a database is to handle information in an integrated manner. There is none of the artificiality that is normally embedded in separate files or applications. A database is collection of interrelated data stored with minimum redundancy to serve many users quickly and efficiently. The general objective is to make information access easy, quick, inexpensive and flexible for the user. In a database environment, common data are available which several authorized users can use. The concept behind a database is an integrated collection of data and provides a centralized access to the data from the program. It makes possible to treat data as a separate resource.

- Controlled redundancy.
- Data Independence.
- More information at low cost.
- Accuracy and Integrity.
- Recovery from failure.
- Privacy and security.
- Performance.

Steps for Dataforge:

1. State what kind of information we need to handle to get the desired output.
2. Find out what information is needed for fields (i.e.) field type, size etc.
3. Remove any data items, which is redundant.
4. Table have one to one relationship needs a primary key field.
5. Tables have one to many relationships needs to add a foreign key field to the table to match the primary key field table.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 03, March 2024, pp: 811-816

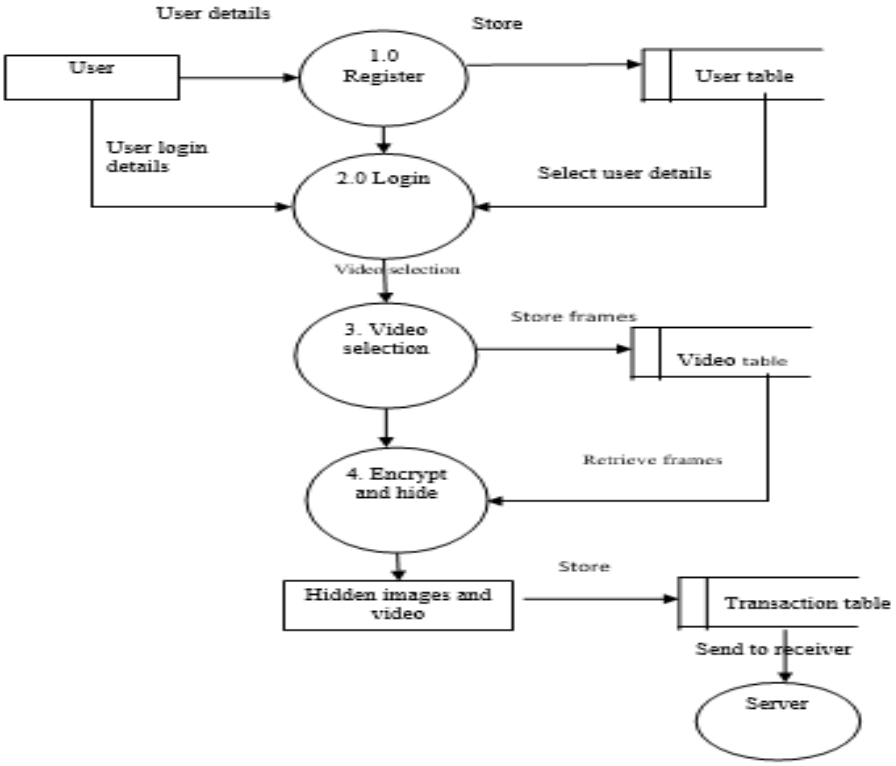

Fig. 1. Level 1 Flow diagram.

Steps for Dataforge:

6. State what kind of information we need to handle to get the desired output.

7. Find out what information is needed for fields (i.e.) field type, size etc.

8. Remove any data items, which is redundant.

9. Table have one to one relationship needs a primary key field.

10. Tables have one to many relationships needs to add a foreign key field to the table to match the primary key field table.

B. Input Design

Input design is one of the most expensive phases of the operation of computerized system and is often the major problem of a system. A larger number of problems with a system can usually be traced back to fault input design and method. The input data is the life block of a system and has to be analyzed with the most consideration.

The decisions made during the input design are: -

- To provide cost effective method of input.
- To achieve the highest possible level of accuracy.
- To ensure that input is understood by the user.

System analysts decide the following input design details like, what data item to input, what medium to use, how the data should be arranged or coded data items and transaction needing validating to detect errors and at last the dialogue to guide users in providing input.

Input data of a system may not be necessarily a raw data captured in the system from scratch. These can also be the output of another system or sub-system. The design of input covers all phases of input from the certain of initial data to actual entering the data to the system for processing.

The design of inputs item capturing and preparing data for computer processing and ensuring correctness of data. Input design is the process of converting user-originated inputs to a computer-based format. Input data are collected and organized into a group of data which are similar. The goal of designing input data is to make data entry easy, logical and free from errors as far as possible.

No command line interface is used in the project. The system is strictly a web-based GUI driven. Special care is given to minimize the data needed to enter by the user. List boxes and option buttons are provided wherever possible.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 03, March 2024, pp: 811-816

C. Output Design

Output design generally refers to the results and information that are generated by the system. For many end-users, output is the main reason for developing the system and the basis on which they evaluate the usefulness of application.The objective of a system finds its shape in terms of the output.

The analysis of the objective of a system leads to determination of outputs. Outputs of a system can take various forms. The most common are reports, screens displays, printed form, graphical drawing etc. the output also vary in terms of their contents, frequency, timing and format. The users of the output, its purpose and sequence of details to be printed are all considered. The output from a system is the justification for it s existence.

If the output is inadequate in any way, the system itself is inadequate. The basic requirements of output are that it should be accurate, timely and appropriate, in terms of content, medium and layout for its intended purpose. Hence it is necessary to design output so that the objectives of the system are met in the best possible manner. The outputs are in the form of reports. When designing output, the system analyst must accomplish things like, to determine what information to be present, to decide whether to display or print the information and select the output medium to distribute the output to intended recipients.

External outputs are those, whose destination will be outside the organization and which require special attention as the project image of the organization. Internal outputs are those, whose destination is within the organization. It is to be carefully designed, as they are the user's main interface with the system. Interactive outputs are those, which the user uses in communication directly with the computer. The output forms of Multi Markup Language Validating System are to view the system's desktop reports.

5. RESULT AND DISCUSSION

Implementation

Implementation is the process of converting a new or revised system design into an operational one. Thus, it can be considered to be the stage in achieving a successful new system and it's vital to assure the user confidence that the proposed new system will never cause impairs and it will be effective. The implementation is not carefully planned and controlled; it can cause chaos. A software application in general is implemented after navigating the complete life cycle method of a project. Various life cycle processes such as requirement analysis, design phase, verification, testing and finally followed by the implementation phase results in a successful project management. The software application which is basically a web-based application has been successfully implemented after passing various life cycle processes mentioned above. As the software is to be implemented in a high standard industrial sector, various factors such as application environment, user management, security, reliability and finally performance are taken as key factors throughout the design phase.

These factors are analyzed step by step and the positive as well as negative outcomes are noted down before the final implementation. The application's validations are made, taken into account of the entry levels available in various modules. Possible restrictions like number formatting, date formatting and confirmations for both save and update options ensures the correct data to be fed into the database.

Thus, all the aspects are charted out and the complete project study is practically implemented successfully for the end users. The approaches of implementation are direct, parallel. In the first approach, the existing system is rejected and the new system is completely implemented. In parallel approach both existing system and new system will be working simultaneously. Direct method of implementation is followed in this project.

6. CONCLUSION

Data security is more important in sensitive command passing environment such as organization secrets, military, government rules and policies should be transmitted securely. The proposed system implements a novel steganography scheme for effective more secure data hiding. The CSST which is abbreviated as random block steganography, which is new storing idea with the use of codeword substitution. Data hiding and encrypting the source media is a new topic that has started to draw attention because of the privacy-preserving requirements in the network domain.

In this project, an algorithm to embed additional data with encrypted data in randomly selected image blocks. Initially the system splits the frame into n number of frames; each block of encrypted secret message will be hidden in the randomly selected block. Finally the system performs the video encryption process which is H.264/AVC bit stream is presented, which consists of video encryption, data embedding and data extraction phases.

7. REFERENCES

[1] Haichao Shi, Xiao-Yu Zhang, Shupeng Wang, Ge Fu, and Jianqi Tang. Synchronized detection and recovery of steganographic messages with adversarial learning. In International Conference on Computational Science, pages 31–43.

[2] Nur Farhana Hordri, Siti Sophiayati Yuhaniz, and Siti Mariyam Shamsuddin. Deep learning and its applications: a review. In Conference on Postgraduate Annual Research on Informatics Seminar, 2016

[3] N. F. Johnson and S. Jajodia. Exploring steganography: Seeing the unseen. Computer, 31(2):26–34, 1998.

[4] Shilpa Gupta, Geeta Gujral, and Neha Aggarwal. Enhanced least significant bit algorithm for image steganography. IJCEM International Journal of Computational Engineering & Management, 15(4): 40–42, 2012.

[5] R. Das and T. Tuithung. A novel steganography method for image based on huffman encoding. In 2012 3rd National Conference on Emerging Trends and Applications in Computer Science, pages 14–18, 2012.

[6] Amritpal Singh and Harpal Singh. An improved lsb based image steganography technique for rgb images. In 2015 IEEE International Conference on electrical, computer and communication technologies (ICECCT), pages 1–4. IEEE, 2015.

[7] Zhiguo Qu, Zhenwen Cheng, Wenjie Liu, and Xiaojun Wang. A novel quantum image steganography algorithm based on exploiting modification direction. Multimedia Tools and Applications, 78(7):7981–8001, 2019.

[8] Shen Wang, Jianzhi Sang, Xianhua Song, and Xiamu Niu. Least significant qubit (lsqb) information hiding algorithm for quantum image. Measurement, 73:352–359, 2015.

[9] Nikhil Patel and Shweta Meena. Lsb based image steganography using dynamic key cryptography. In 2016 International Conference on Emerging Trends in Communication Technologies (ETCT), pages 1–5. IEEE, 2016.

[10] O. Elharrouss, N. Almaadeed, and S. Al-Maadeed. An image steganography approach based on k-least significant bits (k-lsb). In 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), pages 131–135, 2020.

[11] Munthir Bahir Tuieb, Mahmood Zaki Abdullah, and Nazhat Saeed AbdulRazaq. An efficiency, secured and reversible video steganography approach based on lest significant

[12] R. J. Mstafa, K. M. Elleithy, and E. Abdelfattah. A robust and secure video steganography method in dwt-dct domains based on multiple object tracking and ecc. IEEE Access, 5:5354–5365, 2017.

[13] Khalid A Al-Afandy, Osama S Faragallah, Ahmed ELmhalawy, ElSayed M ElRabaie, and Gh M El-Banby. High security data hiding using image cropping and lsb least significant bit steganography. In 2016 4th IEEE International Colloquium on Information Science and Technology (CiSt), pages 400–404. IEEE, 2016.

[14] Anupriya Arya and Sarita Soni. Performance evaluation of secrete image steganography techniques using least significant bit (lsb) method. vol, 6:160–165, 2018.

[15] Gandharba Swain. Very high-capacity image steganography technique using quotient value differencing and lsb substitution. Arabian Journal for Science and Engineering, 44(4):2995–3004, 2019.

[16] Anqi Qiu, Xianyi Chen, Xingming Sun, Shuai Wang, and Wei Guo. Coverless image steganography method based on feature selection. Journal of Information. Hiding and Privacy Protection, 1(2):49, 2019.

[17] Rasber Dh Rashid and Taban F Majeed. Edge based image steganography: Problems and solution. In 2019 International Conference on Communications, Signal Processing, and their Applications (ICCSPA), pages 1–5. IEEE, 2019.

[18] Xin Liao, Jiaojiao Yin, Sujing Guo, Xiong Li, and Arun Kumar Sangaiah. Medical jpeg image steganography based on preserving inter-block dependencies. Computers Electrical Engineering, 67:320–329, 2018.

[19] Wei Lu, Yingjie Xue, Yuileong Yeung, Hongmei Liu, Jiwu Huang, and Yun Shi.Secure halftone image steganography based on pixel density transition. IEEE Transactions on Dependable and Secure Computing, 2019.

[20] Saiful Islam, Aditya Nigam, Aayush Mishra, and Suraj Kumar. Vstegnet: Video steganography network using spatio-temporal features and microbottleneck. 09 2019.