Secure Sharing Information Using Image Audio And Video With Steganography

Raja G[1],SubashChanra Bose P[2],Vijayakumar S[3], SuriyaprakashT[4], Praveern R[5]
[1, 2, 3, 4, 5] Dept of CSE
[1, 2, 3, 4, 5] Dhanalakshmi Srinivasan Engineering College,(Autonomous) Perambalur,T.N,India.

Abstract- *Security is the fundamental requirement for an information society in the distributed network environment. Numerous ways of protecting one's personal or military information are therefore being utilized by individuals, businesses, and governments. When it comes to protecting military data information in images, audio, and video we have developed an information hiding methodology that includes the hiding mechanism based on hiding technique. This project proposed a MSD (Military Secret Data) method which restores the important data. The main aim of data hiding is to enhance communication security by embedding secret messages or audio or video into an inconspicuous carrier and there by transmitting them to receiver. The information is embedded the data that it is perceptually and statistically undetectable. It may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. The basic idea of the methodology was utilizing a high bitrate information hiding technique to embed military information within the actual images, videos and audio files. With this approach, the information was secured and concealed during electronic transmission. This methodology is robust to attacks such as compression, cropping, intrusion, cryptanalysis, etc.*

Keywords- Dot Net, Image Stegnography, Video Stegnography, Audio Stegnography, Common Language Infrastructure (CLI).

I. INTRODUCTION

Steganography is an art of convert communication, which offers secrete and secure way of communication. It has many application areas such as audio-video synchronization, copyright control, TV broadcasting, in defense forces and digital watermarking etc. Broad band internet connections almost an errorless transmission of data helps people to distribute large multimedia files and makes identical data copies of them. Sending sensitive messages and files over the internet are transmitted in an unsecured form but everyone has got something to keep in secret. The aim of steganography is to hide the secret data inside the cover medium without changing the overall quality of cover medium. In steganography actual information is not maintained in its original format but is converted in such a way that it can be hidden inside multimedia file e.g. image, video, audio. The current industries mainly demands for digital watermarking and finger printing of audio and video steganography. The steganography remains intact under transmission and transformation allowing us to protect our secret data. For this the image is converted into bit stream and this bit stream is then embedded in the changing frame. The cybercrimes are also reporting rapidly nowadays hence the steganographic methods should be that much effective and secure so that crimes can be minimized for that cryptography should be combined with steganography for the security of the data come information. The lossless steganography requires storing hidden information in specification location and will requires some time to run the algorithm in order to find the specific location where hidden information can be get stored. Thus, in real time application, the lossless algorithm is becoming tougher to implement, and that depends on the system specifications. The lossy steganography requires storing data at some LSB location or at specific pixel locations. This is easy to implement and it can be apply in real time application with any normal system specifications. The LSB (Least Significant Bit) is used here to hide the data. The first frame is selected as index frame and it contains the information regarding where the information is stored, in which form information is getting stored, what is file type of the information, etc information are stored in the index frame.

II. IDENTIFY,EXISTING SYSTEM

Existing System

Over the past years an enormous variety of different chaos-based image and video encryption algorithms have been proposed and published. While any algorithm published undergoes some more or less strict experimental security analysis, many of those schemes are being broken in subsequent publications. In this work we show that two main motivations for preferring chaos-based image encryption over classical strong cryptographic encryption, namely computational effort and security benefits, are highly questionable. We demonstrate that several statistical tests, commonly used to assess the security of chaos-based

encryption schemes, are insufficient metrics for security analysis. We do this experimentally by constructing obviously insecure encryption schemes and demonstrating that they perform well and/or pass several of these tests. In conclusion, these tests can only give a necessary, but by no means a sufficient condition for security. As a consequence of this work, several security analyses in related work are questionable; further, methodologies for the security assessment for chaos-based encryption schemes need to be entirely reconsidered.

Disadvantages

- The traditional way is followed to compare the original and encrypted image where the changing intensity value is found to be typically lower.
- Complexity is more.
- Distortion is high
- Only analysed the audio steganography

Proposed System

The proposed work will focus on hiding information in specific frames of the by Discrete Wavelet Transform (DWT) Compression and Least Significant Bit (LSB) substitution and AES. The proposed method uses images, audio and video based steganography because of large size and memory requirements. The system can hide the text using three way such as image, audio and video steganography. Proposed system will support large size audio file. When uploading large audio files that will be splited into multiple part and hide individually on different cover files. The video is converted into frames. Frames are splitted for every 0.05 secs. Then these frames are compressed using DWT Haar compression technique. The frame that should be used to hide the audio data is selected. Then the hiding of the audio data in the selected frame is done by LSB insertion technique. After data embedding, the frames are decompressed using inverse DWT compression. The frames are rejoined to form the steganographed video. This video will look alike the original video. But few changes will be made. This can't be identified by human eyes. This will be sent to the receiver.

Advantages

- DWT mechanism assures complete security of the secret image, video and audio.
- LSB achieves high embedding capacity compared with other data hiding techniques.
- Computational complexity is low.

SOFTWARE SUMMARY

FRONT END

.NET FRAMEWORK

The .NET Framework (pronounced dot net) is a software framework developed by Microsoft that runs primarily on Microsoft Windows. It includes a large library and provides language interoperability (each language can use code written in other languages) across several programming languages. Programs written for the .NET Framework execute in a software environment (as contrasted to hardware environment), known as the Common Language Runtime (CLR), an application virtual machine that provides services such as security, memory management, and exception handling. The class library and the CLR together constitute the .NET Framework.

The .NET Framework's Base Class Library provides user interface, data access, database connectivity, cryptography, web application development, numeric algorithms, and network communications. Programmers produce software by combining their own source code with the .NET Framework and other libraries. The .NET Framework is intended to be used by most new applications created for the Windows platform. Microsoft also produces an integrated development environment largely for .NET software called Visual Studio.

BACK END

SQL SERVER

Microsoft SQL Server is a relational database management system developed by Microsoft. As a database server, it is a software product with the primary function of storing and retrieving data as requested by other software applications—which may run either on the same computer or on another computer across a network (including the Internet). Microsoft markets at least a dozen different editions of Microsoft SQL Server, aimed at different audiences and for workloads ranging from small single-machine applications to large Internet-facing applications with many concurrent users. Data storage is a database, which is a collection of tables with typed columns. SQL Server supports different data types, including primary types such as Integer, Float, (including character strings), Varchar (variable length character strings), binary (for unstructured blobs of data), Text (for textual data) among others.

SQL Server scales from a portable tablet to symmetric multiprocessor frameworks.

SQL Server gives information warehousing elements that as of recently have just been accessible in Oracle and other more costly DBMSs.

Elements of SQL Server

Microsoft SQL Server bolsters a full arrangement of elements that outcome in the accompanying. SQL incorporates an arrangement of managerial and advancement instruments that enhance our capacity to introduce, convey, oversee and use SQL Server over a few locales.

Adaptability

The same database motor can be utilized crosswise over stages going from smart phones Microsoft Windows95 to substantial; multiprocessor servers running Microsoft Windows NT, Enterprise Edition.

Ease in building information distribution centers

SQL Server incorporates instruments for removing and examining synopsis information for online investigative preparing (OLAP). SQL Server likewise incorporates apparatuses for outwardly planning databases and breaking down information utilizing English based inquiries.

III. WRITEDOWNYOUR STUDIESANDFINDINGS

IMPLEMENTATION

Software testing is a method of assessing the functionality of a software program. There are many different types of software testing but the two main categories are dynamic testing and static testing. Dynamic testing is an assessment that is conducted while the program is executed; static testing, on the other hand, is an examination of the program's code and associated documentation. Dynamic and static methods are often used together.

Testing is a set activity that can be planned and conducted systematically. Testing begins at the module level and work towards the integration of entire computers based system. Nothing is complete without testing, as it is vital success of the system.

I. Testing Objectives:

There are several rules that can serve as testing objectives, they are

1. Testing is a process of executing a program with the intent of finding an error
2. A good test case is one that has high probability of finding an undiscovered error.
3. A successful test is one that uncovers an undiscovered error.

If testing is conducted successfully according to the objectives as stated above, it would uncover errors in the software. Also testing demonstrates that software functions appear to the working according to the specification, that performance requirements appear to have been met.

There are three ways to test a program

1. For Correctness
2. For Implementation efficiency
3. For Computational Complexity.

Tests for correctness are supposed to verify that a program does exactly what it was designed to do. This is much more difficult than it may at first appear, especially for large programs.

Tests used for implementation efficiency attempt to find ways to make a correct program faster or use less storage. It is a code-refining process, which reexamines the implementation phase of algorithm development. Tests for computational complexity amount to an experimental analysis of the complexity of an algorithm or an experimental comparison of two or more algorithms, which solve the same problem.

The data is entered in all forms separately and whenever an error occurred, it is corrected immediately. A quality team deputed by the management verified all the necessary documents and tested the Software while entering the data at all levels. The development process involves various types of testing. Each test type addresses a specific testing requirement. The most common types of testing involved in the development process are:

• Unit Test.
• Functional Test
• Integration Test

3.1 Unit Testing

The first test in the development process is the unit test. The source code is normally divided into modules, which in turn are divided into smaller units called units. These units have specific behaviour. The test done on these units of code

is called unit test. Unit test depends upon the language on which the project is developed. Unit tests ensure that each unique path of the project performs accurately to the documented specifications and contains clearly defined inputs and expected results.

3.2 Functional Testing

Functional test can be defined as testing two or more modules together with the intent of finding defects, demonstrating that defects are not present, verifying that the module performs its intended functions as stated in the specification and establishing confidence that a program does what it is supposed to do.

3.3 Integration Testing

In integration testing modules are combined and tested as a group. Modules are typically code modules, individual applications, source and destination applications on a network, etc. Integration Testing follows unit testing and precedes system testing. Testing after the product is code complete. Betas are often widely distributed or even distributed to the public at large in hopes that they will buy the final product when it is released.

IV. CONCLUSION

There are various kinds of steganography techniques available to hide data in image, audio and video format. In our approach, DWT compression along with LSB substitution is used. Large size audio file has been splited into multiple parts. Some specific key is used to hide the data. That specific key is too used to store the data as a background of the frames. Once receiver gets no video then merge shares. The above mentioned approach is used to hide a data into an image audio and video file which provides a robust and secure way of data transmission. The proposed embedded video steganography has many advantages like user friendliness, simple and successful process of embedding secret message with more security.

V. FUTURE ENHANCEMENT

In future, this method can be tested with other wavelet transform techniques with various image quality measurements and also implemented for videos of more length in less amount of time and will generate large amount of storage in the server.

REFERENCES

[1] M. IndraSena Reddy, Dr. A.P. Siva Kumar," Secured Data Transmission Using Wavelet Based Steganography and Cryptography by Using AES Algorithm", International Conference on Computational Modeling and Security, Procedia Computer Science, Vol: 85, 2016, pp: 62 – 69.

[2] Marwa M. Emam, Abdelmgeid A. Aly, Fatma A. Omara, "An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection", International Journal of Advanced Computer Science and Applications, Vol: 7, Issue: 3, 2016, pp: 361 - 366.

[3] Ramandeep Kaur, Pooja, Varsha, "A Hybrid Approach for Video Steganography using Edge Detection and Identical Match Techniques" , International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 2016, pp: 896 - 900.

[4] Yingnan Zhang, Minqing Zhang, Xiaoyuan Yang, DuntaoGuo and Longfei Liu, "Novel Video Steganography Algorithm Based on Secret Sharing and Error-Correcting Code for H.264/AVC", TSINGHUA SCIENCE AND TECHNOLOGY, Vol : 22, Issue: 2, 2017, pp: 198 - 209

[5] Ramadhan J. Mstafa, Khaled M. Elleithy and EmanAbdelfattah, "A Robust and Secure Video Steganography Method in DWT-DCT Domains Based on Multiple Object Tracking and ECC", IEEE Access, Volume: 5, 2017, pp: 5354 - 5365.