Asian Journal of Applied Science and Technology (AJAST)
(Peer Reviewed Quarterly International Journal) Volume 2, Issue 4, Pages 246-254, Oct-Dec 2018

An Efficient Data Hiding Using Steganography and Cryptography for Audio, Image and Video Files

P.Shamly[1] & R.Senthilkmar[2]

[1]*PG Scholar, Department of Computer Science and Engineering, Shree Venkateshwara HiTech Engineering College, Erode, Tamilnadu, India.*
[2]*Assistant Professor, Department of Computer Science and Engineering, Shree Venkateshwara HiTech Engineering College, Erode, Tamilnadu, India.*

Article Received: 19 June 2018 *Article Accepted: 28 October 2018* *Article Published: 09 December 2018*

ABSTRACT

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. For hiding secret information in audio, there exists a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. Different applications have different requirements of the steganography technique used. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden. This project intends to give an overview of audio and text steganography, its uses and techniques. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography. Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret. Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated. Existing algorithms does it. On the basis of drawbacks in existing system we proposed LSB scheme for high level security and accuracy in stenography The scheme exploits the brightness, edges, and texture masking of the host image to estimate the number k of LSBs for data hiding. Pixels in the noise non-sensitive regions are embedded by a k-bit LSB substitution with a lager value of k than that of the pixels in noise sensitive regions. Moreover, an optimal pixel adjustment process is used to enhance stego-image visual quality obtained by simple LSB substitution method. To ensure that the adaptive number k of LSBs remains unchanged after pixel modification, the LSBs number is computed by the high-order bits rather than all the bits of the image pixel value. Transfer the encrypted output audio from source to destination over LAN. After reached destination the audio must be extracted with proper key. Many steganographic systems are weak against visual and statistical attacks. Systems without these weaknesses offer only a relatively small capacity for steganographic messages. The newly developed algorithm LSB withstands visual and statistical attacks, yet it still offers a large steganographic capacity. LSB implements matrix encoding to improve the efficiency of embedding. Thus it reduces the number of necessary changes. LSB employs permutative straddling to uniformly spread out the changes over the whole steganogram..

Keywords: Steganogaphy, data hiding, LSB and Cryptography.

1. INTRODUCTION

Communication is an indispensable part of life. With the advent of digital technology, this has become more sophisticated than ever before. Moreover, information has become in a sense the most expensive and valuable commodity in today's world. In addition, the rapid growth of the computer era has led to all documentations, audio and video being digitized. This has increased the necessity for ensuring the security and integrity of any document, audio and video to maintain privacy, piracy and mass reproduction. There are many categories of information such as business, research, finance and many more. This information is traded between the countries and states for various purposes which require Information Security. Information Security is the only solution which gives us secure information and therefore a secure communication. Information security plays a pivotal role to keep the information safe. Though several successful methods exist for Information Security, they are still in research to boost up their performance. Undoubtedly, Information Security is a soul of exchange of data. Information Security systems are classified into two categories namely Information encryption and Information hiding. These two methods are used to protect the information. Information Encryption and Data hiding techniques were found in Bender et al (1996) and Peticolas et al (1999). Figure 1.1 shows the classification of the security systems.

2. PROBLEM STATEMENT

The amount of convenient Apps has created at a huge rate over the span of late years. To quicken the progression of adaptable Apps, Many App stores impelled each day App pioneer sheets, which show the framework rankings of most standard Apps. A superior rank on the pioneer board when in doubt prompts a huge number of downloads and million dollars in wage. As opposed to relying upon regular advancing courses of action, shady Apps architects swing to some phony method to purposefully bolster their Apps and at last control the diagram rankings on an Apps store. For that we propose to develop a situating distortion revelation structure for compact Apps. Indeed, our attentive discernment reveals that compact Apps are not continually situated high in the pioneer board, but instead just in some leading events, which outline differing leading sessions. Figuratively speaking, situating distortion generally happens in these dynamic sessions. Specifically, we at first propose a direct yet convincing computation to recognize the principle sessions of each App reliant on its certain situating records. By then, with the examination of Apps situating hones, we find that the tricky Apps as often as possible have different situating precedents in each leading session differentiated and normal Apps.

3. LITERATURE REVIEW

Communication has become inevitable in everybody's routine life. Be it e-mails, text, or photo or audio, video, they get communicated in millions among billions. There are many categories of information such as business, research, finance, etc. This information is traded between the countries and states for various purposes which require secure communication. Information security is the only solution which can give us secure information and help us to have a secure communication. Information security plays a pivotal role to keep the information safe. Among the prominent definitions for information security, the most vital of them is information security which is about veracity, discretion and data availability. Though several successful methods exist, they are still in research to boost up their performance. Undoubtedly, information security is a soul of exchange of data. Steganography is the popular security method that provides complete security for communicating secret details. Image steganography is a very interesting field because of the imperceptible way of hiding data in images, since small distortion in the images cannot be identified by a human eye. This is the main idea to develop image steganography algorithms for secure communication. Image Steganography can be done either in spatial domain or in transform domain. LSB (Least Significant Bit) Embedding is a technique for embedding secret information into a cover image. A Mathematical model for LSB technique has been developed by Chan and Cheng (2004) for embedding and extracting the secret data. PVD (Pixel Value Differencing) is another efficient technique for spatial domain steganography, which provides high data embedding capacity with reasonable PSNR.

All the spatial domain steganography techniques are using this LSB substitution technique for embedding the secret data. Chan and Cheng (2004) proposed a data hiding scheme by simple LSB substitution with an Optimal Pixel Adjustment Process (OPAP). In general, OPAP is used to improve the stego image quality with low computational complexity. In this method, first LSB to fourth LSB is changed according to the secret message. PSNR values are

varying from 51dB to 34dB. Adaptive LSB steganography is proposed by Yang et al (2009). In this technique, Image is divided into sensitive and non-sensitive area based on the texture analysis. High number of bits is embedded in the non-sensitive area and minimum number of bits is embedded in the sensitive area. Such adaptive embedding scheme provides security against blind steganalysis, high embedding capacity and high imperceptibility. Yang (2008) discovered a new technique for LSB steganography. LSB substitution approach embeds the secret messages into the LSB of the cover pixels. But in this method large secret messages are inverted and then embedded into the cover pixel (1000 to 0001). The experimental results are reported with high PSNR for high payload.

4. OBJECTIVES

The main objective of this Research work is to implement Adaptive and Non-Adaptive Random image Steganography with very high security by enhancing the Complexity, Capacity and Imperceptibility in addition to the minimized key length.

Implementation of Spatial Domain Random Image Steganography using Pixel Value Differencing and Knight's Tour in Digital images.

Implementation of adaptive and non-adaptive Random Image Steganography in Integer Wavelet Transform Domain (IWT) by using Haar and 5/3 (IWT). Implementation of adaptive and non-adaptive Random Image Steganography in Integer Wavelet Transform Domain (IWT) using Graph Theory and Knight's Tour.

5. ARCHITECTURE DIAGRAM

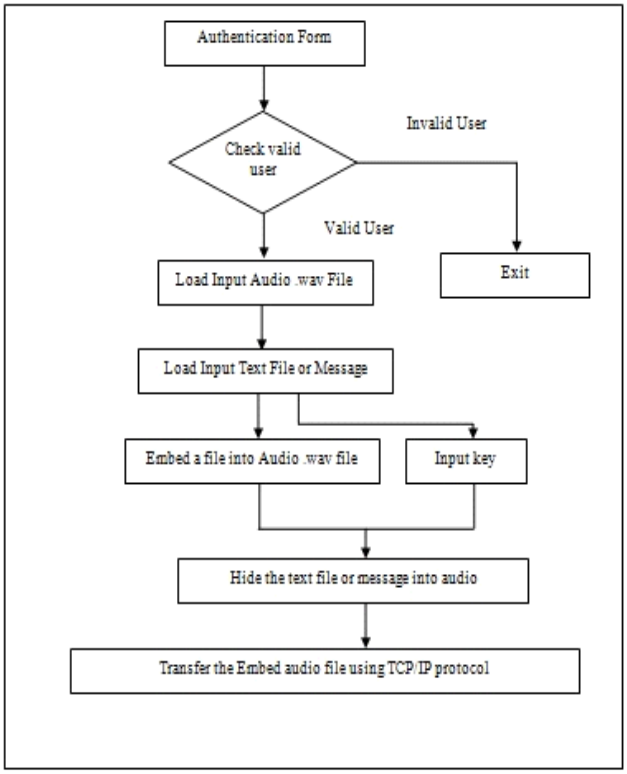

Fig.1. Architecture Diagram

 Online ISSN: 2456-883X

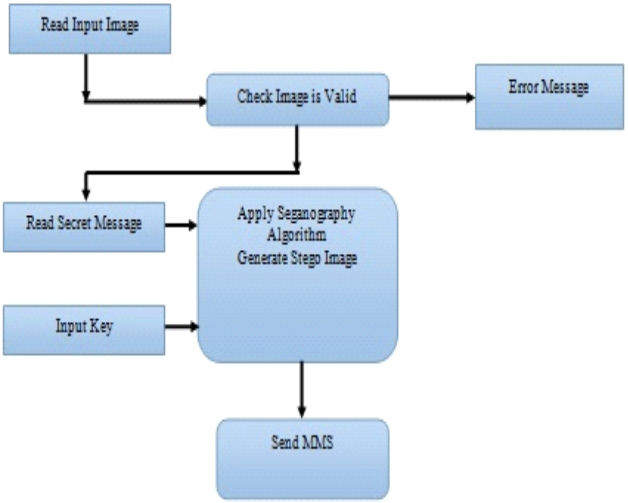

Fig.2. Sender Side Flow Diagram

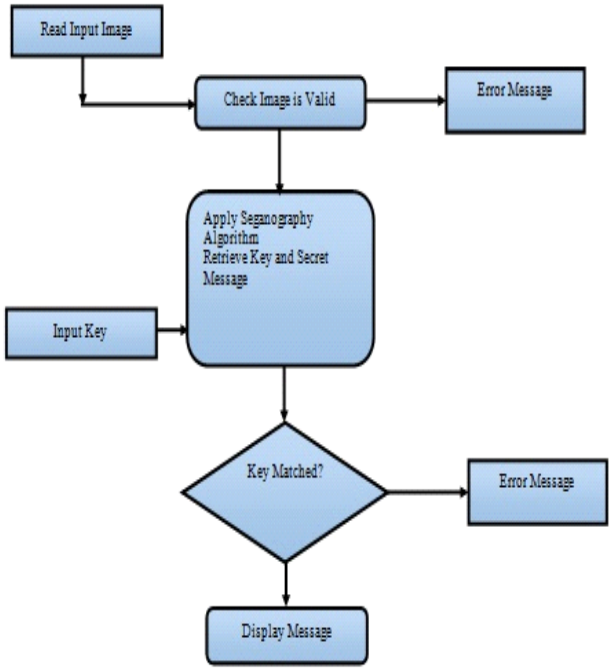

Fig.2. Receiver Side Flow Diagram

6. RESEARCH METHODOLOGY

6.1 AUDIO STEGANOGRAPHY

Steganography can be applied to audio files. Audio files may be modified in such a way that they contain hidden information in such a way that it is difficult to remove the hidden data without destroying the original signal. Audio steganography takes advantage of the psycho acoustical masking phenomenon of the human auditory system (HAS). The HAS perceives the additive random noise and also the perturbations in a sound file can also be detected. While the HAS have a large dynamic range, it has a fairly small differential range. As a result, loud sounds tend to mask out quiet sounds. And there are also some distortions that are so common that the HAS ignores them.

6.2 EXISTING SYSTEM

In existing system to hide the data normally using cryptography method, encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information (in cryptography, referred to as cipher text). In many contexts, the word encryption also implicitly refers to the reverse process, decryption (e.g. "software for encryption" can typically also perform decryption), to make the encrypted information readable again (i.e. to make it unencrypted).

Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret. Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated. Existing algorithms does it. On the basis of drawbacks in existing system, propose F5 algorithm for high level security and accuracy in image stenography for android application.

6.3 Disadvantages

Existing method approach to map secret data to one of the three channels of the RGB image. The proposed method uses the idea of transposition, bitxoring, bits shuffling, secret key, and cryptography to design an advanced steganographic system. Unlike other methods, the proposed method have the following multiple security levels. 1) All the three channels of the input carrier image are transposed before they can be used to map secret data in order to deceive the attacker. 2) The secret key and secret data is encrypted using multiple encryption algorithms that are applied on it one after another. 3) Secret data is mapped to blue channel of the carrier image using gray-level modification method (GLM). The proposed method uses two different modules named as encryption module and mapping module in order to hide secret data to the carrier image pixels.

6.4 PROPOSED SYSTEM

Steganography is a technique to hide secret messages in a host media called cover media. The advantage of Steganography over cryptography is that messages do not attract attention to attackers and even receivers. Steganography and cryptography are often used together to ensure security of the secret messages. Steganography and Cryptography are parallel data security techniques, both techniques can be implemented side by side, in fact most steganographic utilities implements cryptographic data security. While the two fields aren't contradicting each other they have different qualities.

- Steganography can use cryptography but not the other way around.
- With cryptography we can protect the message but not hide its existence.
- Steganography has a very expensive payload as compared to cryptography.

Hiding a message in Wave samples is very similar to hiding it in the pixels of a bitmap. Again, we use a key stream to skip a number of carrier units (samples/pixels), grab one carrier unit, put one bit of the message into the lowest bit of the carrier unit, and write the changed unit to the destination stream. When the entire message has been hidden like that, we copy the rest of the carrier stream.

6.5 Points of interest

Our goal is to build an android application for image stenography that is able to send and receive encrypted messages with respect to image stenography through MMS. When people initially tried to communicate over distances, they tried to ensure the secrecy of their communications. The android technology based image steganography developed for this objective.

.

7. TESTING AND IMPLEMENTATION

7.1 BASIC MODULES

Testing is a series of different tests that whose primary purpose is to fully exercise the computer based system. Although each test has a different purpose, all work should verify that all system element have been properly integrated and performed allocated function. Testing is the process of checking whether the developed system works according to the actual requirement and objectives of the system. The philosophy behind testing is to find the errors. A good test is one that has a high probability of finding an undiscovered error. A successful test is one that uncovers the undiscovered error. Test cases are devised with this purpose in mind. A test case is a set of data that the system will process as an input. However the data are created with the intent of determining whether the system will process them correctly without any errors to produce the required output.

7.2 SYSTEM TESTING

It is the stage of implementation, which ensures that system works accurately and effectively before the live operation commences. It is a confirmation that all are correct and opportunity to show users that the system must be tested with text data and show that the system will operate successfully and produce expected results under expected conditions. Software testing is a crucial element of software quality assurance and represents the unlimited review of specification, design and coding. Testing represents an interesting anomaly for the software. During the earlier definition and development phase, it was attempted to build the software from an abstract concept to tangible implementation.

7.3 INTEGRATION TESTING

The entire project was split into small program; each of these single programs gives a frame as an output. These programs were tested individually; at last all these programs where combined together by creating another program where all these constructors were used. It give a lot of problem by not functioning is an integrated manner.

The user interface testing is important since the user has to declare that the arrangements made in frames are convenient and it is satisfied. When the frames where given for the test, the end user gave suggestion. Based on their suggestions the frames where modified and put into practice..

7.4 VALIDATION TESTING

At the culmination of the black box testing software is completely assembled as a package. Interfacing errors have been uncovered and corrected and a final series of test i.e., Validation succeeds when the software function in a manner that can be reasonably accepted by the customer.

7.5 OUTPUT TESTING

After performing the validation testing the next step is output testing of the proposed system. Since the system cannot be useful if it does not produce the required output. Asking the user about the format in which the system is required tests the output displayed or generated by the system under consideration. Here the output format is considered in two ways. One is on screen and another one is printed format. The output format on the screen is found to be corrected as the format was designed in the system phase according to the user needs. And for the hardcopy the output comes according to the specifications requested by the user.

8. SYSTEM IMPLEMENTATION

The purpose of System Implementation can be summarized as follows:

It making the new system available to a prepared set of users (the deployment), and positioning on-going support and maintenance of the system within the Performing Organization (the transition). At a finer level of detail, deploying the system consists of executing all steps necessary to educate the Consumers on the use of the new system, placing the newly developed system into production, confirming that all data required at the start of operations is available and accurate, and validating that business functions that interact with the system are functioning properly. Transitioning the system support responsibilities involves changing from a system development to a system support and maintenance mode of operation, with ownership of the new system moving from the Project Team to the Performing Organization.

List of System implementation is the important stage of project when the theoretical design is tuned into practical system. The main stages in the implementation are as follows:

- Planning
- Training
- System testing and
- Changeover Planning

Planning is the first task in the system implementation. Planning means deciding on the method and the time scale to be adopted. At the time of implementation of any system people from different departments and system analysis

involve. They are confirmed to practical problem of controlling various activities of people outside their own data processing departments. The line managers controlled through an implementation coordinating committee. The committee considers ideas, problems and complaints of user department, it must also consider;

- The implication of system environment
- Self-selection and allocation form implementation tasks
- Consultation with unions and resources available

Standby facilities and channels of communication.

9. CONCLUSION

A simple text hiding scheme has been introduced. However, it greatly enhances the effectiveness of the Steganography since it uses a key, making it much more challenging to detect. In the end we found both effective, but the complexity of bit-o-steg makes it more promising. Detection of our methods was critical to the breadth of our project. By investigating the power in various components of our images we discovered how to detect data hidden via the zero hiding method. Detecting bit-o-steg required us to draw on past Steganography research and statistically analyze the effects of this type of data hiding. The methods and accompanying detection schemes we developed broadened our understanding of Steganography, which, unlike encryption, allows secret data to be traded hands without raising an eyebrow.Steganography can be applied to different types of media including text, audio, image and video etc. Now that we have hidden data in bitmaps, MIDI tracks and Java assemblies, you might miss one important file format. You might miss the files that can hide lots of bytes without becoming larger, and can be generated in a few seconds, so that you don't have to store the original files on your disk. It is time to add Wave Audio to the list. So we did it successfully using wav files.

REFERENCES

[1] S. K. Subramaniam, S. H. Husin, R. S. S. Singh and A. H. Hamidon, "Production Monitoring System for Monitoring the Industrial Shop Floor Performance", *International Journal of Systems Applications, Engineering & Development*, Issue 1, Volume 3, 2009.

[2] S. K. Subramaniam, S. H. Husin, Y. Yusop, A. H. Hamidon, "Data collection using a real time production monitoring system for factors affecting production lines", *Journal of Science and Technology in the Tropics* (2008) 4 Page(s):129-134.

[3] Killeen, D., Gaboury, P. & Paccard, D., "Managing, measuring and improving equipment capacity and overall equipment efficiency (OEE) using iPLUS", *IEEE International Semiconductor Manufacturing Symposium, 8-10 Oct 2001*, Page(s): 25 – 28.

[4] Tom Pherson, June 2006, 'Overall Equipment Effectiveness & Real-Time Visual Management Critical Lean Tools' *Intelligent Manufacturing Solutions*, Page(s):1-18.

[5] Ashwini Deshpande Prajakta and Pitale Sangita Sanap, "Industrial Automation using Internet of Things (IOT)", *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, Volume 5 Issue 2, February 2016.

[6] Li Da Zu, "Internet of Things in Industries: A Survey" *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, November 2014.