PROVIDING A SECURE DATA HIDING AND EXTRACTION SYSTEM USING BPCS

Jakduva Usman Hasan, Kadatskaja O.

V.V. Popovsky Departanent Infocommunication Engineering,
Kharkiv National University of Radio Electronics, Ukraine

E-mail: usman.hassan.jakduwa@nure.ua,
olha.kadatska@nure.ua

Abstract

The aim of this article is to address the issue of insecurity faced by users communicating over the internet. This will be achieved by providing a secure data hiding and extraction system using bit-plane complexity segmentation. With the successful implementation of this solution, the security of messages sent via the internet will be ensured.

Information Technology is the most essential aspect in today's world. Based on this fact computer application is still developing to handle securely the financial as well as the personal data more effectively. These data are extremely important from every aspect, and we need to secure this from unauthorized access. Security is the process of preventing and detecting unauthorized use of data or computer or network. Prevention measures help us to stop unauthorized users from accessing any part of computer system.

Prevention measures and detecting unauthorized use of data, computer or network help us to stop unauthorized users from accessing any part of computer system [1]. Detection helps to determine whether someone attempted to break into the system, if they were successful, and what they may have done. To achieve that security, we may use various cryptography techniques. However, today data encryption is not everything or we cannot achieve strong security through this, we also need to secure the presence of data and comes the necessity of steganography. But that neither cryptography nor steganography gives the total security to a data or information uniquely, thus we need to apply both techniques to achieve essential security. There are number of ways this can be done, but here we will focus on methods of altering the information in such a way that the recipient can undo the alteration and discover the original text.

Steganography and cryptography there are some notable and distinctive differences between the two. In some situations, steganography is often preferred to cryptography because in cryptography the cipher text is a scrambled. output of the plaintext and the attacker can guess that encryption has been performed and hence can employ decryption techniques to acquire the hidden data. Also, cryptography techniques often require high computing power to perform encryption which may pose a serious hindrance for small devices that lack enough computing resources to implement encryption.

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal, is the process of hiding digital information in a carrier signal, the hidden information does not need to contain a relation to the carrier signal [2]. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. Like traditional watermarks, digital watermarks are only perceptible under certain conditions, i.e., after using some algorithm, and imperceptible anytime else. If a digital watermark distorts the carrier signal in a way that it becomes perceivable, it is of no use. Traditional Watermarks may be applied to visible media (like images or video), whereas in digital watermarking, the signal may be audio, pictures, video, texts or

3D models. A signal may carry several different watermarks at the same time. Unlike metadata that is added to the carrier signal, a digital watermark does not change the size of the carrier signal. The needed properties of a digital watermark depend on the use case in which it is applied. For marking media files with copyright information, a digital watermark must be rather robust against modifications that can be applied to the carrier signal. Instead, if integrity must be ensured, a fragile watermark would be applied. Both steganography and digital watermarking employ steganographic techniques to embed data covertly in noisy signals. But whereas steganography aims for imperceptibility to human senses, digital watermarking tries to control the robustness as top priority. Since a digital copy of data is the same as the original, digital watermarking is a passive protection tool. It just marks data but does not degrade it nor controls access to the data. A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later, then the watermark may be retrieved from the copy and the source of the distribution is known. Digital watermarking may be used for a wide range of applications.

A bitmap (BMP) image will be used to hide the data. Data will be embedded inside the image using the pixels. Then the pixels of stegoimage can then be accessed back in order to retrieve back the hidden data inside the image. Data privacy issues can arise from healthcare records, criminal justice investigations and proceedings, financial institutions and transactions, biological traits, residence and geographic records and ethnicity. Data security or data privacy has become increasingly important as more and more systems are connected to the Internet. There are information privacy laws that cover the protection of data or information on private individuals from intentional or unintentional disclosure or misuse. Thus, hiding the data in a kind of form such as within an image is vital in order to make sure that security or privacy of the important data is protected.

In data hiding, famous techniques can be used as a steganography and cryptography. Other forms of data hiding involve the use of tools and techniques to hide data throughout various locations in a computer system. Some of these places can include memory, slack space, hidden directories, bad blocks, alternate data streams and hidden partitions. Steganography is hiding the existence of a message by hiding information into various carriers. The major intent is to prevent the detection of hidden information. Steganography is a technique where information or files are hidden within another file in an attempt to hide data by leaving it in plain sight. There are several steganography techniques used for hiding data such as batch steganography, permutation steganography, least significant bits (LSB), bit-plane complexity segmentation (BPCS) and chaos based spread spectrum image steganography (CSSIS).

Cryptography is for secure communication constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Encrypted messages can sometimes be broken by cryptanalysis, also called codebreaking, although modern cryptography techniques are virtually unbreakable. Messages to be sent will be hidden inside a picture file using the data hiding software. This file can then be attached to the current messaging service and sent to the recipient. Upon receiving the picture file through the message attachment, the recipient uses their copy of the data hiding software to view the hidden message in the picture file.

The new system will be designed using the Microsoft Visual Basic Programming Language for its implementation. The data to be used by the system will be managed using the Microsoft Access database. Below are the descriptions and structure of the database files to be used by the system. User info file, this database file will contain the information about the users allowed to use the solution. The dataflow diagram shows the flow of data between the user of the system, the processes and the system's data storage points. Using Donathan Hutchings algorithm implementation is created he dataflow diagram of the new system.

Donathan Hutchings image data hiding algorithm embeds the text inside a graphic file and creates a key file to be used to read the message later.

- Input in algorithm are Image File, Secret Message.

- After determining the size of the Image File and the length of the Secret Message determine the offset to use when embedding the Secret Message. This gives a reliable starting position based on the sizes of the Image File and Secret Message.
- Need place secret message bytes in key data array stores the locations of each Secret Message byte and store the location of the whole Secret Message byte and create a new Image File with the Secret Message inside.
- Create the file key.
- The output file will be Stego_Image.

The message reading algorithm is stored in a graphic file. Now the input data for the algorithm is the file Stego_Image. Determined the size of the Image File the length of the Secret Message. After need read the Image File byte data into a byte array and message location data from the key file. From the Image File data find message and construct our actual Secret Message. Get the message byte from the Image File data. Convert the byte data back to our original Secret Message. The output will be a file Secret Message.

To implement this system a parallel approach plan will be used Based on Donathan Hutchings Algorithm developed a system which implements the algorithm. Based on the framework for the system, the first layer is for the login purpose and the second layer is for the hiding, retrieving of message purposes and lastly viewing hidden message file details interface. The image file format used in this study is focused on bitmap (BMP) format. BMP files is the simplicity and wide acceptance of BMP files in windows programs. Since BMP image has a relatively large size, the pixels in image are relatively larger as well. Thus, it provides more space for binary codes to be encoded within it. To increase as much as characters that can be hidden, in this new system, has been tested several sizes of BMP images to see the various sizes of data being stored in the image. Received various results for the testing   and also shows the comparison of different sizes in BMP image by using the steganographic software.

The successful implementation of this study will ensure that the results of this study can be used by in the field of data information security, the results of this research will increase the level of confidentiality of information exchanged over the internet, access to information by malicious individuals such as hackers will no longer be possible as they will be unable to locate which form of media was used to hide the information and government monitoring will be impossible as information hidden in other forms of media will go undetected by them.

In this article been conducted research on secure data hiding and extraction using BPCS. Amongst the objectives includes the Design a solution that will enable the storage of data in picture media using steganography data hiding techniques and the implementation and testing of the solution to ensure that it conforms to the objectives set out by the researcher.

Conclusion

The proposed Data Hiding System will be very essential to the privacy and security of messages sent through the as they will be hiding in multimedia files. Once the inefficiencies of communicating through the current messaging systems are solved, it is hoped that the achievement will lead researchers and computer scientist to find ways to ensure the security of information exchanged over the other communication technologies that exist over the internet.

References

1. Bandyopadhyay, S. Roy.*"Information Security through Data Encryption and Data Hiding"*. International Journal of Computer Applications (0975 – 8887) Volume 4– No.12,2010.

2. Nosrati, A. Nosrati, “Embedding stego-text in cover images using linked list concepts and LSB technique”, Journal of American Science, Vol. 7, No. 6, 2011.

3. Cory J., 2014. [Online] Available: http://www.techopedia.com/definition/14738/data-hiding, http://searchsqlserver.techtarget.com/definition/data-hiding