IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-1, Dec 2019 E-ISSN: 2347-2693

Implementation of Email System With Steganography

Uzair Nisar[1*], Craig Stewart[2]

[1,2]Department of Computing, Coventry University, Coventry, United Kingdom

[*]*Corresponding Author: uzair.bhat@live.com, Tel.: +91-9906806346*

Available online at: www.ijcseonline.org

Accepted: 22/Jan/2019, Published: 31/Jan/2019

***Abstract*—** Email Systems are widely used as the means of communication. Organizations in order to seek more security tend to lean towards more secure ways of communication. This project facilitates the means of communication in a more secure format. The system being developed uses the technique called 'Steganography'. Steganography hides the data behind an image so any intruder or hacker can only see the image and not the critical data. This is the secure means of sending information. To make it even more secure the steganographic image is then protected by a password using the technique called 'Cryptography'. This can be implemented by developing 3 tools, first of which will hide data behind image, then the next tool encrypts it with a password and the final tool is used to send it over internet. This system will not only provide the best secure communication of data but it also makes the use of three different tools embedded in a single system.

Keywords*—AES,LSB,Steganography,Cryptography*

I. INTRODUCTION

Email is the modern means of communication and plays a very important role in our life. Most of the people use computers to check their emails which are often related to their day to day work or other formal issues. Email service is provided by various organizations like Microsoft, Yahoo, Google etc. but none of them provide a secure system for transferring critical data.

The Email system being developed will not only embed the voice feature in future for reading out emails in your inbox but will also include a modern encryption technique to secure the critical data that is to be transmitted over the network. A well implemented system like this can provide number of benefits to the customer and business. A system like this is can be uploaded on the organization's servers to run over their network and most organizations use TLS SSL to secure their transmission from intrusion. Keeping that in mind an idea of securing the system with the means of "Steganography" seems appropriate. It is a process in which we send our file or data with an image covering it for the view. That means a hacker can only see the image but not the important file in the background. So, this feature embedded in this system would allow organizations to send and receive data in emails without any intrusion. This system is accessible from anywhere in the world and since it would be setup on the organizations server it can be used even if there is no internet connection.

This paper is organized as: Related work done with the Email systems and Steganography was discussed in Section II. The proposed methodology, flow of data and coding used were mentioned in Section III. The implementation algorithm for Steganography and Cryptography were mentioned in Section IV. Conclusion of the paper with future directions were mentioned in Section V and VI respectively.

II. RELATED WORK

Email systems and Email servers use TLS & SSL to secure the transmission of data online. Email providers like Gmail, Yahoo, Outlook they provide TLS & SSL [1] encryption over Transport and Session layer of the TCP/IP model. This provides a secure channel between client and server so as to transfer data securely without any intrusion. This form of encryption is being used by all email service providers. But there is a catch, what if somebody hacks into the network? He can easily access the critical data thus breaching the security. The idea I came up with is the other form of securing the critical data in this system or network and that is using Steganography. This form of security has never been used in any email service before and may result in being more effective. The positive aspect in this is that even if some hacker breaks into the network he/she will not be able to find the critical data, because Steganography teaches us hiding the data over another data. So, the hacker would be looking at simple data files in the network but he/she would not have any idea that the critical data is being stored and transmitted in the background of these data files present. This will not only help the final product to be good in secure transmission but will also keep the file secured till the authorized person accesses it.

A. Steganography

Hiding information in other information when communication is taking place is usually referred as steganography. Digital images are the most popular among different file formats available on internet because of their frequency. Many stenographic techniques are available for information hiding. All of these have their respective positive and negative points. Various steganography techniques are used in different applications based on their requirements. For example, absolute invisibility may be required by some applications to hide secret information, whereas others require to hide large secret messages. [2] presented different image steganography techniques overview and also explain which techniques prove useful to what applications.

Another technique called Cryptography was created for securing communication but unfortunately it fails to keep the message secret. What it does is it encrypts the message using some algorithm and puts on a password to the data but it does not hide the existence of data if anybody gets the key, he can view all the information. But steganography makes message existence a secret. According to [3] the word steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" showing that is a technique for "covered writing". Information can be hidden in images by image steganography. This technique is used by computers for communication under secure environment. The model of steganography includes a Carrier, Message to be sent and the Password kept. Carrier is a cover-object, used for sending the secure data in the hidden form. Message is the secure data we want to send and could be in form of text, image or embedded data. Password is known as stego-key, which is used to extract the secure data from the cover object at the recipient's end. Below figure shows the model for steganography.

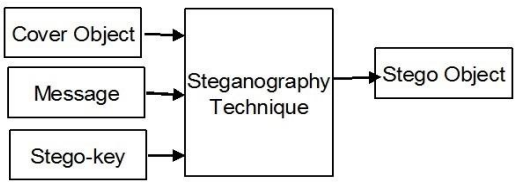

Figure 1. Basic Steganography Model

According to [4] steganography is different from cryptography, in cryptography the message is kept secret whereas in steganography the existence of message is secret. In this project I have used both of these technologies to secure information thus the strength of security can be improved.

Steganography uses digital file formats with a high degree of redundancy. According to [5] redundancy is the bits of an object which provide more accuracy than necessary for objects used and displayed. An object redundant bit can be easily altered without detection of alteration. Four main file format categories that form the type of steganography are shown in the following figure.

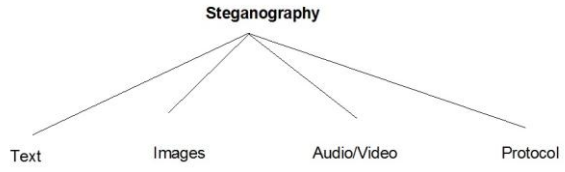

Figure 2. Steganography Categories

Historically the most used method of steganography was hiding information in text. As very small amount of expendable data is present in text files, text steganography which uses digital file is not used very often. In steganography images are depicted as popular cover objects. Audio files uses same techniques as image files to hide information. Masking is the technique that is specific to audio steganography and is not used for image files. This technique is developed by [2] in which a low but distinct sound becomes faint in the presence of another distinct louder sound. A channel is created by this property for information hiding. According to [6] vast size of important sound documents almost equivalent to pictures in stenographic potential make them less prevalent to use than pictures. Conventional steganography is a system in which data is implanted inside of messages and system control conventions utilized as a part of transmission [7]. The header of TCP/IP packet may contain hidden information that is either optional or never used.

Pictures are most famous items utilized for steganography. Distinctive stenographic calculations exist for diverse picture document designs. Generally, picture is accumulation of numbers speaking to diverse light intensities at distinctive regions. These numbers form a grid and each point is referred as pixel. Images on internet are displayed in form of rectangular map of image pixels. These pixels are represented as bits and are displayed in a row by row manner horizontally. Colour of each pixel is described by 8 bits. These 8 bits can display 256 shades of grey in monochrome and greyscale images. 24-bit file is used to store digital colour images and uses RGB colour model. Red, green and blue are three primary colours used to derive all variations of a 24-bit image. 8 bits are utilized to speak to every essential shading, along these lines in one pixel there are 256 distinct measures of every essential shading and subsequently making 16-million blends bringing about more than 16-million colours.

1) Advantages

The benefit of steganography over cryptography is that messages don't draw in consideration regarding themselves. Obviously unmistakable scrambled messages regardless of

how unbreakable will stir suspicion, and may in themselves be implicating in nations where encryption is unlawful while as though we utilize steganography there is no suspicion. Thusly, while cryptography secures the substance of a message, steganography can be said to ensure both messages and imparting gatherings.

- Watermarking images is done for example for the reason such as copyright protection.
- Tagging notes to online images.
- Maintaining the confidentiality of valuable information.
- It is attained by some modern-day printers, like HP and Xerox.
- Steganography in audio can be used with mobile phone.
- It helps in the protection of data being altered.
- Access control system for digital content distribution.
- Used with Media Database systems.
- Peer to Peer private communications.

2) Disadvantages

Steganography being highly secure can however additionally possess significant issues on the grounds that it's hard to identify. System observation and checking frameworks won't banner messages or documents that contain steganographic information. Subsequently, on the off chance that somebody endeavoured to take secret information, they could hide it inside another document and send it in a blameless looking email. For instance, if someone was trying to steal data, they could conceal it in another file or files and send it out in an innocent looking email or file transfer.

- Moreover, a man with a side interest of sparing explicit entertainment, or more regrettable, to their hard drive, may decide to shroud the proof through the utilization of steganography.
- It can be utilized as a method for clandestine correspondence.
- Sending remote Trojans to people in order to get the access of their computers.
- If hacker gets to know that the image sent on a network carries a message file, he can perform steganalysis to extract the message.

III. METHODOLOGY

The product would be developed following the Spiral model. The process is done while keeping in mind the requirements and objectives of the product and is designed accordingly. The product will be built module by module and each module will be tested and evaluated before going on to the next module. After some analysis and research of what is to be done, we start building up the product using C# language in Visual Studio. The design is made according to the requirements. Implementation of the system is completely code based and it will contain both design and business logic in it. Other than that, the product would carry a database where all the data and files for the system would remain saved.

A. Data Flow Diagram

The data flow diagram below shows the complete representation of how data flows throughout the system. An overview of the system can be clearly obtained.

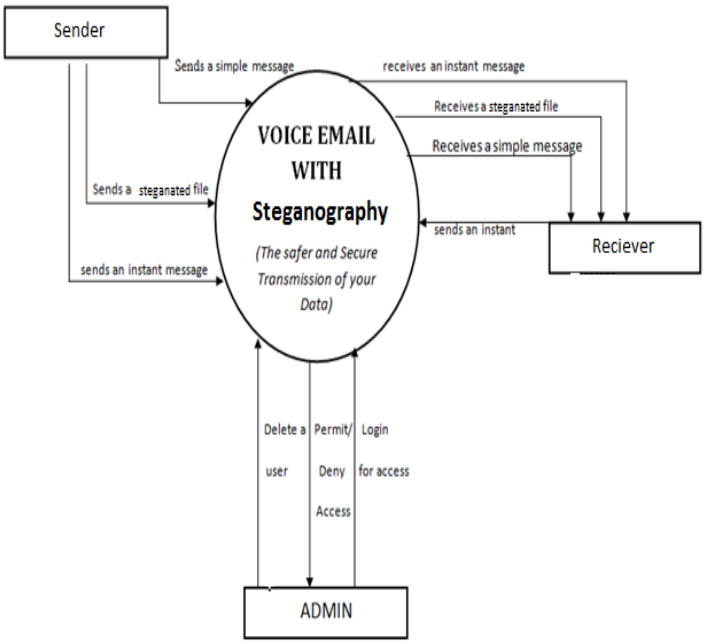

Figure 3. Context Level DFD

IV. IMPLEMENTATION

The logic for the project is based on two main important modules that are explained below:

A. Steganography Module

The logic behind this module is done using the image steganography technique called Least Significant Bit method or LSB [8]. Steganography can be attained by different methods like image, audio, text, video but the most used and practiced technique is through image steganography. In image steganography Least Significant Bit method is used. In this method the least bit of an image is altered and the data to be hidden is stored in those bits. Since it is called least significant bits so by changing those bits in an image the

image view is not tampered. Inside every image there is RGB colour combination, we take one pixel of the image of 3 bytes for Red and Green and Blue of 8 bits each. Every byte last bit is taken out and data is put in these. The data to be put is first converted into binary. LSB uses .bmp images because they use lossless compression. LSB method explained by an example below:

Grid of 3 pixels of a 24bit image can be written as
(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

When 200 whose binary representation is 11001000 is embedded in the least significant bits of the part of the image, the resulting grid is as follows:

(00101101 00011101 11011100)
(10100110 11000101 00001100)
(11010010 10101100 01100011)

Example of how it works practically, can be seen in the figure below:

Original Image Message File Stego Image

Figure 4. Stegnation Process

The alteration done by editing the least significant bits of the image to put in the message is not visible to the naked eye.

B. *Cryptography Module*

The algorithm used in this system to secure the data with a password is "Rinjdael" Algorithm [9] or AES (Advanced Encryption Standard) and we have used 256-bit symmetric encryption. Made by "John Daemon" and "Vincent Rijmen," two Belgian cryptology experts. The U.S. National Bureau of Standards created a complicated encryption standard called DES (Data Encryption Standard) which offered unlimited ways to encrypt data. This encryption standard was replaced by "Rijndael" encryption because of its versatility and highly complex nature.

In Rijndael data is put in 4 by 4 table of bytes, which is called 'State'. It has 10, 12 and 14 rounds depending on the bit size either 128 or 192 or 256. Below figure explains the steps of encryption performed using this method.

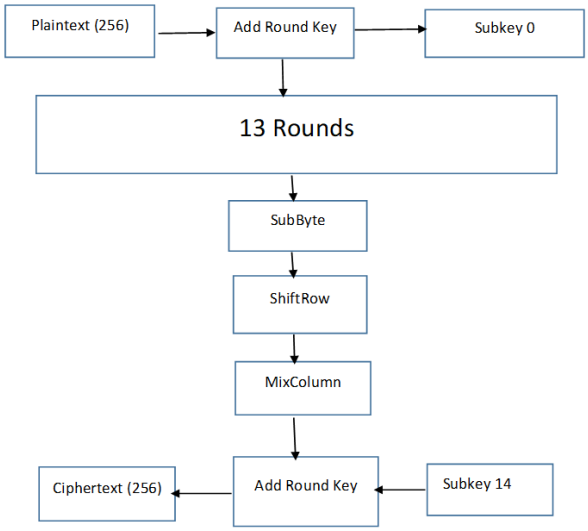

Figure 5. AES Design Flow for 256 bits

C. *AES Decryption*

In AES decryption the steps done are in the reverse order as that of done for encryption. All the rounds and transformations are same but the data feed in this is the cipher text which gives out the plain text in the result.

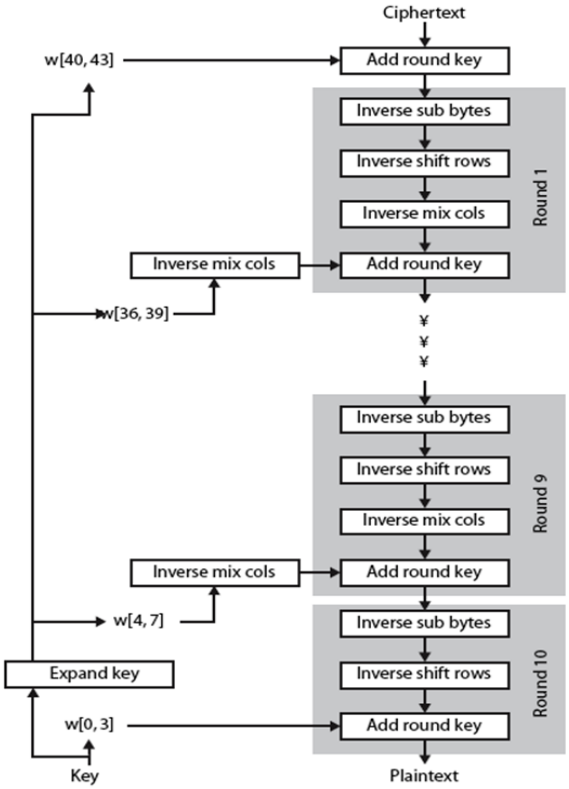

Figure 6. AES Decryption

V. CONCLUSION

The implementation of this experiment produces a sound and secure email system for an organization which will be secured under the cryptographic encryption called "Rijndael" [9] and the data sent will be hidden using the technology called Steganography. This project uses image steganography to hide the data inside the image. This technique is attained through LSB [8] (Least Significant Bit) method. The system will not only be secure but will also be the only one of its kind being made. Adding to that, this system will have a Voice feature to read and write emails so that it will become hands-free. This System is developed using C# coding language keeping in view the hypothesis and methods attained in the research study. The results proving the hypothesis will only be confirmed after the development stage. This can be done by testing the system and putting it in use to perform the said operation. The system should successfully deliver the aim and objectives it is meant to deliver.

The result of this experiment will be a system, the only one of its kind that will perform the work of three different tools. This can be used by security agencies and other organizations for the safer communication of the data.

VI. FUTURE WORK

Steganography is the new technology and it still has not been researched that much. It is mostly done with the image but future enhancements include text, video, files etc. There are consistent progressions in the PC field, recommending headways in the field of steganography also. It is likely that there will soon be more productive and more propelled systems for Steganalysis because the process of Steganography is getting more advanced and very difficult to detect and due to that fact, it can have an important application of hiding important government data and likewise can prove harmful too. A cheerful headway is the enhanced affectability to little messages. Knowing that it is so hard to distinguish the vicinity of a genuinely extensive content record inside of a picture, envision that it is so hard to recognize even maybe a couple sentences inserted in a picture. It is similar to discovering a minute needle in a definitive sheaf.

This system, once accepted by users has a scope of being upgraded into a full-fledged email system on web. In future it can also incorporate in automated systems that can read an email and generate an auto response based on the content of the email. The interface of the system developed can gain a lot of advancements and styles for better look and usability. Moreover, the full-fledged email system with steganography and cryptography included can get more accurate with timely updates in the algorithms.

ACKNOWLEDGMENTS

All the praise to almighty Allah my head bows in humble towards him for He blessed me with the strength and courage to accomplish this task. I fall short of words to pen down anything for the co-operation and encouragement extended by my parents on every step of my life. Not to forget I am also very thankful to my project supervisor Dr Craig Stewart who helped me with this project.

REFERENCES

[1] Stephen Thomas, 'SSL and TLS essentials', Securing the web, **2000**.

[2] Morkel, T., Eloff, J. H., and Olivier, M. S, "An overview of image steganography", In ISSA, pp.**1-11, 2005.**

[3] Moreland, T, 'Steganography and Steganalysis', Leiden Institute of Advanced Computing Science, **2003.**

[4] Wang, H. and Wang, S, 'Cyber warfare: steganography vs. steganalysis'. Communications of the ACM, 47(10), pp**.76-82**, **2004**

[5] Currie III, D. L., & Irvine, C. E. 'Surmounting the effects of lossy compression on Steganography',NAVAL POSTGRADUATE SCHOOL MONTEREY CA DEPT OF COMPUTER SCIENCE, **1996.**

[6] Artz, D, 'Digital steganography: hiding data within data', internet computing, IEEE, 5(3), pp. **75-80, 2001**.

[7] Ahsan, K., and Kundur, D, 'Practical data hiding in TCP/IP', InProc. Workshop on Multimedia Security at ACM Multimedia (Vol. 2, No. 7) December, **2002**.

[8] K. Nandhini, B. Gomathi, 'Open Access Article Implementation of LSB Based Steganography Algorithms in FPGA, Research Paper Journal (IJSRNSC), Vol.6 , Issue.5 pp.**32-37, Oct-2018**

[9] Ferguson, N., Kelsey, J., Lucks, S., Schneier, B., Stay, M., Wagner, D., & Whiting, D, 'Improved cryptanalysis of Rijndael'. In Fast software encryption January pp. **213-230**,**2001**.

[10] Garfinkel, S. L, 'Public key cryptography', Computer, 29(6), pp.**101-104**, **1996.**

[11] Sarmah, D. K., and Bajpai, N. 'Proposed System for data hiding using Cryptography and Steganography', in International Journal of Computer Applications, 8(9), pp**. 7-10**, **2010**.

[12] Johnson, N. F., and Jajodia, S. 'Exploring steganography: Seeing the unseen', Computer, 31(2), pp. **26-34**, **1998.**

[13] Geer, D, 'Taking steps to secure web services', Computer, 36(10), pp**. 14-16, 2003.**

[14] Sunner, M, 'Email security best practice', Network Security, pp**. 4-7**, **2005.**

[15] Levi, A., and Koç, Ç. K, 'Inside risks: Risks in email security', .Communications of the ACM, 44(8), 112, **2001.**

[16] JJTC, Steganography. Technical Report [online] available from http://www.jjtc.com/pub/tr_95 _11_nfj/sec401.html 29 November **2015.**

[17] Salomon, D, 'Data privacy and security: encryption and information hiding'. Springer Science & Business Media, **2003.**

[18] Katzenbeisser, S., and Petitcolas, F, 'Information hiding techniques for steganography and digital watermarking'. Artech house, **2000.**

[19] Westfeld, A, 'Steganography for radio amateurs—A DSSS based approach for slow scan television'. In Information Hiding January pp**. 201-215**, **2007.**

[20] Codr, J. (2009). 'Unseen: An Overview of Steganography and Presentation of Associated Java Application C-Hide'. Retrieved January, 8, **2010.**

[21] Anderson, R.J. and Petitcolas, F.A, 'On the limits of steganography'. Selected Areas in Communications, IEEE Journal on, 16(4), pp.**474-481**, **1998**.

[22] Harshal V. Patil1, B. H. Barhate, 'Open Access Article A Review Paper on Data Hiding Techniques: Stegnography, Review Paper Journal Paper (IJSRCSE), Vol.06 , Special Issue.01, pp**.64-67, Jan-2018.**

Authors Profile

Mr. Uzair Nisar pursued Bachelor of Technology (B. Tech) from Islamic University of Science and Technology, Kashmir India in 2014 and Master of Science from Coventry University, UK in year 2016. He is EC Council Certified Ethical Hacker and has worked with Microsoft India under their two different student programs, Microsoft Student Partner and Windows Ucrew respectively from the year 2012 to 2014. Mr Uzair has over 2 years of experience in Network Management and System Administration. He has also been awarded the 2nd position in an IT quiz at a national level.

Dr Craig Stewart pursued Bachelor of Science in Genetics from Nottingham University, UK, Master of Science in Molecular Genetics from University of Leicester and PHD in Computer Science from University of Nottingham. He is currently working as the Lecturer for the MSc in Digital Games and Business Innovation at the Serious Games Institute, Coventry University. Dr Stewart has worked in the area of HCI, IT & multimedia research and education for over 20 years. He has a great deal of experience in many fields from working in various departments, disciplines and positions. Dr Stewart's doctoral research (entitled A Cultural Education Model: Design and Implementation of Adaptive Multimedia Interfaces in eLearning) consists of examining the effect that TEL is having on cultural education and how HCI impacts on this.

