International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

An Efficient Technique of Steganography

Latika[1], Yogita Gulati[2]

[1]M-Tech Scholar, PIET College, Panipat, Haryana, India

[2]Research Guide, PIET College, Panipat, Haryana, India

Abstract: ***This paper presents a Steganography Technique that uses DES (Data Encryption Algorithm), to encipher and decipher the blocks of data, which is based on symmetric key algorithm that uses a 56 bit key. By applying this algorithm we have developed an application that helps the user to hide their secret or a confidential data. Along with it we have used a compression technique that will increase the storage capacity.***

Keywords: Steganography, DES (Data Encryption Standard), Cryptography, conceal system, extraction, embedding, symmetric key, encryption, decryption, cipher text, symmetric key

1. Introduction

Steganography is defined as the system of hiding secret or a confidential data in a cover media like image, text, video, audio, in such a way that none other than the intended recipient knows the presence of data. Markus Kahn [1] as follows, "Steganography is the art and science of communicating in a way which hides the existence of the communication. In contrast to Cryptography, where the enemy is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present".

In this digital world, both the concepts i.e. the cryptography and steganography hides the data from the unintended recipients or an intruder. Due to this fact, the authors prefer a multilayer security by combining the benefits of both. The steganography concept can be implemented through various formats available worldwide. Various formats preferred are .jpeg, .gif, .mp3, .doc, .docx. Due to ease of availability of these formats on the internet, they are preferred to hide the secret message. Steganography research has been driven because of weakness in the cryptography systems those results in the security breach. Many tools and technologies created takes advantage of steganography techniques like coding in image, null ciphers, videos, audio, etc

2. A brief history of Steganography

The concept of steganography came in to existence in 440 BC by the Greek historian Herodotus. [2]He recorded two stories of steganography techniques during this time. The first one is Darius of Susa shaved the head of one of his prisoners and wrote a secret message on his scalp. When the prisoner's hair grew back, he was sent to the Kings son in law Aristogoras in Miletus undetected. The second story claims that a soldier named Demeratus needed to send a message to Sparta that Xerxes intended to invade Greece. Back then, the writing medium was text written on wax-covered tablets. Demeratus removed the wax from the tablet, wrote the secret message on the underlying wood, recovered the tablet with wax to make it appear as a blank tablet and finally sent the document without being detected. In a similar way [2] Romans used invisible inks which were based on natural substances. In Century 15 & 16 two writers wrote on steganography techniques. Between 1883 and 1907, two writers Auguste Kerckhoff (author of Cryptographic Militaire) and Charles Briquet (author of Les Filigranes), attributed to the further development in the field of steganography. At the times of world wars first and second, different concepts were developed in the field of steganography like null cipher, coding in images. In this modern era, experts prefer to use a mix of steganography and cryptography techniques i.e. combining the benefits of both the technologies to provide a secure communication between the sender and the recipients. This ensures a multilayer security and thus the obtained system is more robust.

3. Steganography Terms

The terminologies used in the field of steganography are cover image, stego image, message and a stego key. The terms can be further explained below:

- **Cover Image:** A carrier of secret information.
- **Stego Image:** The image which is obtained after embedding secret message in a cover image is termed as Stego Image
- **Message:** The original message which is to be hidden.
- **Stego Key:** To embed and retrieve the original data through embedding and retrieving algorithm respectively, the stego key is required.

4. General Steganography Approach

The concept of steganography can be described in terms of sender, receiver, both extracting and embedding algorithms, and secret key. The idea can be formulated as:

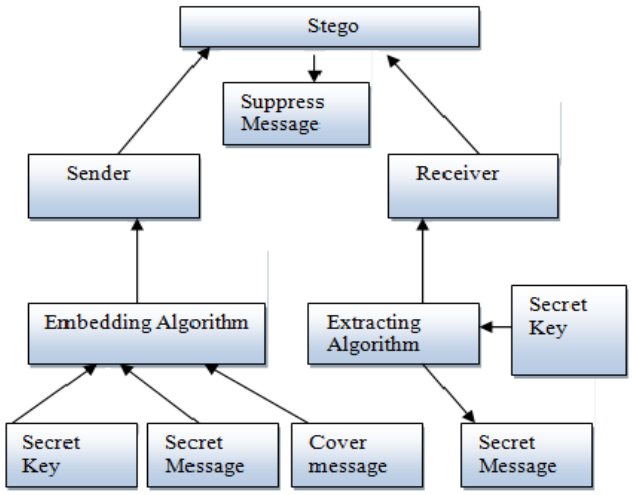

Figure 1: Steganography System [3]

5. Proposed System

In the proposed system, first we will give the message to be secured in to the proposed system i.e. Conceal and Secure System. Then, the system will return the message secured under an image cover.

In the Conceal and Secure system, we will make a function F in which we will take an image cover C, secret message M, and a key image K. This function will return a stego image S at the client side. When this message is sent to the receiver side, then private key will be given to him. When the private key will match, then stego image will open. The image folder, key image, and the secret image will remove .Thus a receiver can get the message in secure format by using Conceal and Secure System.

The DES algorithm is used is based on a symmetric-key algorithm that uses a 56-bit key. The algorithm was initially controversial because of classified design elements, a relatively short key length, and suspicions about a National Security Agency (NSA) backdoor. DES consequently came under intense academic scrutiny which motivated the modern understanding of block cipher and their cryptanalysis. The Conceal and Secure System can be further explained through a diagram as designed below:

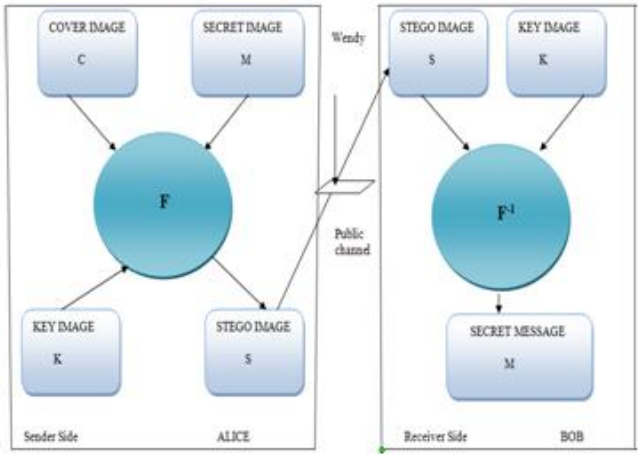

Figure 2: Conceal and Secure System

6. A detailed Look to the proposed System

1) After the successful compilation of the code, we get the screen figure 4.
2) For Embedding Purpose, we need to go to the file and then click on the options "*Go for Embedding*".
3) The obtained screen contains the source file, through which the sender will upload the image. Along with it the sender has to specify the destination file where the stego image will be saved. We have also used the concept of compression and password. So the sender has to click on the checkbox for compression and has to provide a password, which is only known to the sender and receiver. (Figure 5)
4) When we click on embedding , the message "*embedding done successfully*" is displayed as shown below: (figure 6)
5) After embedding, the process of de-embedding starts. In this screen, the Receiver has to upload a stego image received from the sender. The receiver has to provide the password, if the password matches with the one applied by the sender, then deem bedding is done. (figure 7)

7. Result Analysis

Result analysis of conceal and secure system is given below. With the help of this system we take six result and these are following:

Here we explain the first result of Conceal & Secure System which is mentioned above- In first case we take a 176kb source image, 13kb text message, and 4kb text file. After perform CSS steps (i.e. compress, encrypt, embed, decrypt, & de-embed) we take result and in this result we found that source image size reduce and it becomes 175.45kb but we get the message successfully i.e. is 13kb. Similarly we take rest of results.

Table 1: Result Analysis

S.no	*Sender Side*			*Receiver Side*	
	Source image(size)	*Text Message (size)*	*Text File*	*Image (size)*	*Text Message (size)*
1.	170 Kb	13 Kb	4 Kb	170Kb	13 Kb
2.	176 Kb	45 Kb	6 Kb	175.45Kb	45 Kb
3.	145 Kb	54 Kb	5 Kb	144.34Kb	54 Kb
4.	166 Kb	34 Kb	6 Kb	165.7Kb	34 Kb
5.	155 Kb	44 Kb	5 Kb	154.56Kb	44 Kb
6.	140 Kb	45 Kb	8 Kb	139.45Kb	45 Kb

8. Implementation in Java

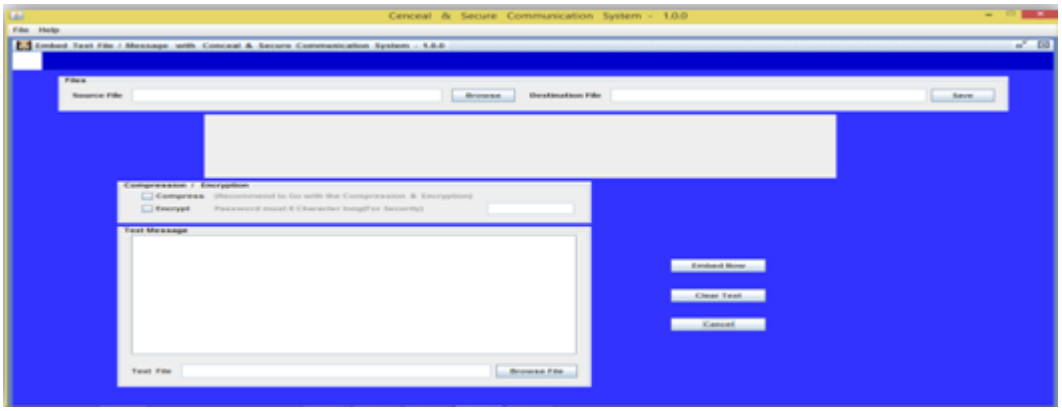

Figure 4: Main Screen

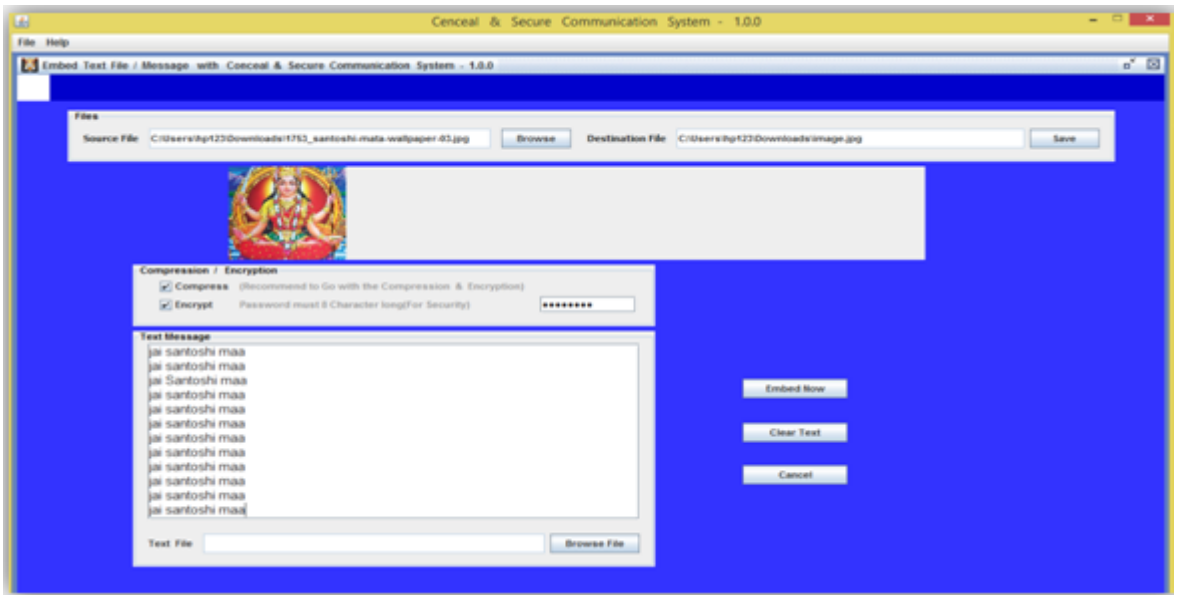

Figure 5: Screen for embedding

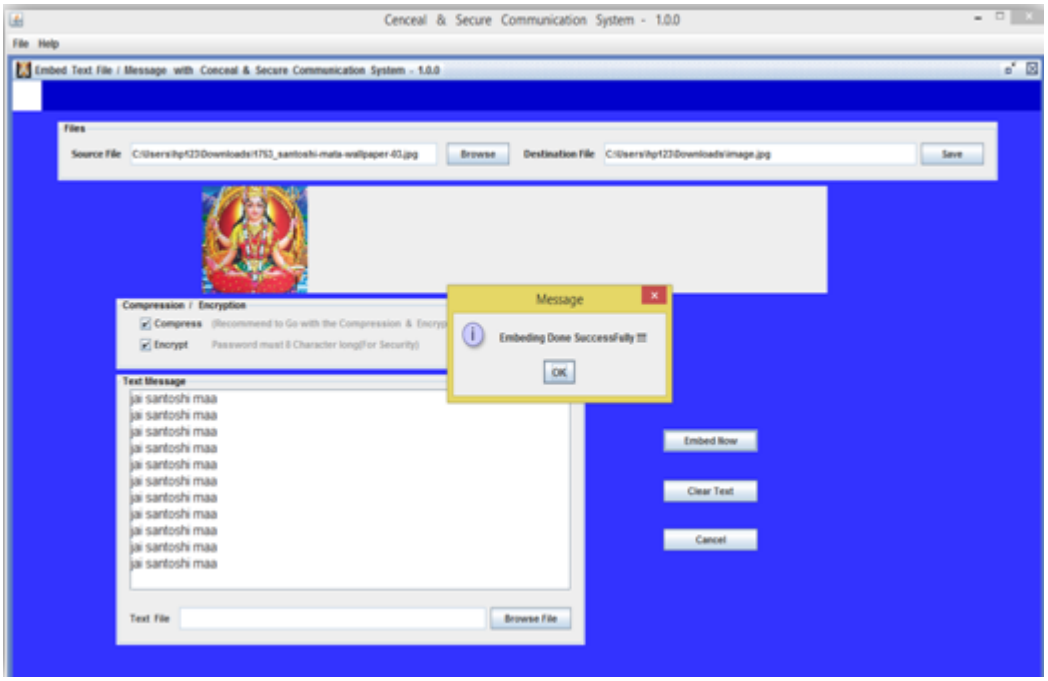

Figure 6: Embedding Done successfully

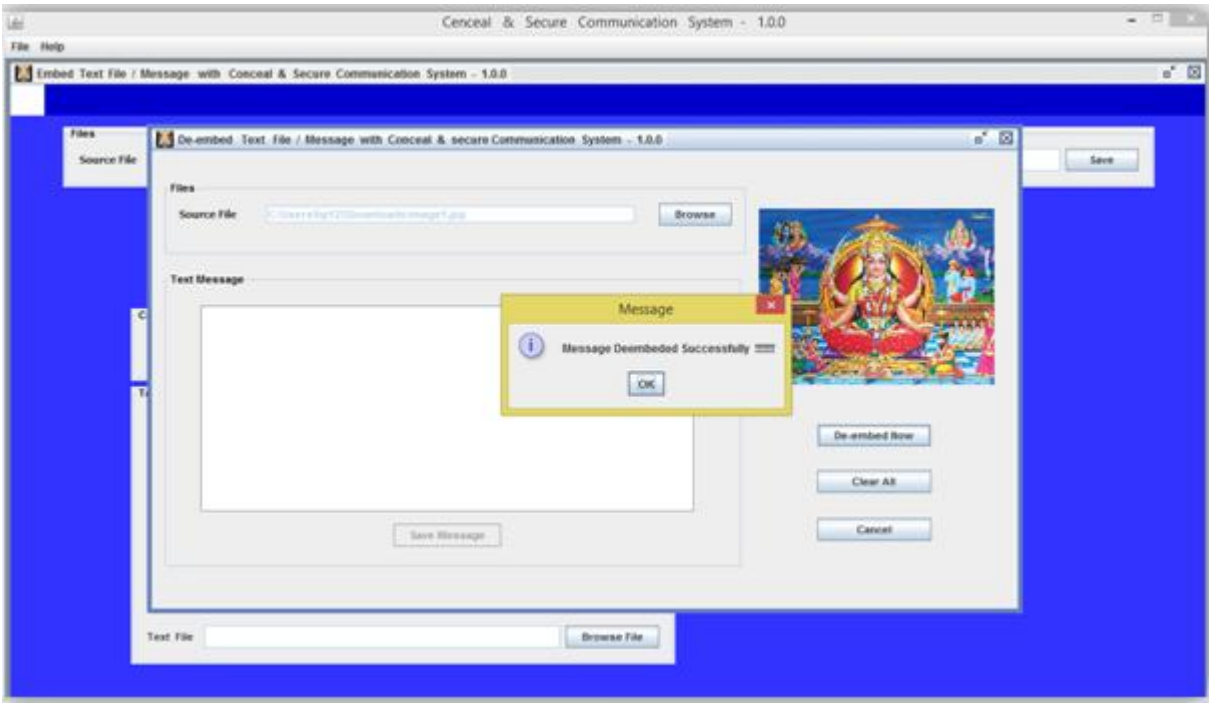

Figure 7: Screen for De-embedding

9. Conclusion

In this paper, we have developed a new steganography technique that allows the sender to embed the secret data in the cover image through a password, which is known only to the sender and receiver. The receiver provides the password and gets the secret data intended to him. Here, we have developed a proposed system in java using the said algorithm. Here we have also used a compression algorithm that will increase the storage capacity. Thus the Steganography technique proposed is more robust and very efficient for hiding text .

10. Future Scope

The Steganography techniques will continue to increase in popularity over the cryptography. There are various future scopes in hiding the secret data in audio and video formats. There is also a scope in developing a system which is a combination of the merits of both techniques.

References

[1] Johnson, Neil F., "Steganography", 2000, URL: http://www.jjtc.com/stegdoc/index2.html
[2] B. Dunbar. A detailed look at Steganographic Techniques and their use in an Open-Systems Environment, Sans Institute, 1(2002).
[3] Latika and Yogita Gulati," A Comparative Study and Literature Review of Image Steganography Techniques" IJSTE - International Journal of Science Technology & Engineering | Volume 1 | Issue 10 | April 2015.
[4] Gowtham Dhanarasi and Dr.A. Mallikarjuna Prasad "Image Steganography using Block Complexity Analysis" International Journal of Engineering Science and Technology (IJEST) Vol. 4 No.07 July 2012
[5] Rahul Jain and Naresh Kumar "Efficient data hiding scheme using lossless data compression and image steganography" International Journal of Engineering Science and Technology (IJEST) Vol. 4 No.08 August 2012.
[6] Siddharth Singh and Tanveer J. Siddiqui "A Security Enhanced Robust Steganography Algorithm for Data Hiding" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, May 2012.
[7] Hemalatha S1, U Dinesh Acharya, Renuka A, Priya R. Kamath "A secure and high capacity image steganography technique "An International Journal (SIPIJ) Vol.4, No.1, February 2013
[8] Vipul Sharma and Sunny Kumar "A New Approach to Hide Text in Images Using Steganography" International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 4, April 2013.
[9] Dipesh Agrawal and Samidha Diwedi Sharma "Analysis of Random Bit Image Steganography Techniques "International Journal of Computer Applications (0975 – 8887) International Conference on Recent Trends in engineering & Technology - 2013(ICRTET'2013)."
[10] Kumar, R. And Chand, S." A new image steganography technique based on similarity in secret message" Confluence 2013: The Next Generation Information Technology Summit (4th International Conference) IET.
[11] Ashima Wadhwa "A Survey on Audio Steganography Techniques for Digital Data Security "International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 4, April 2014.
[12] Dagar, S. "Highly randomized image steganography using secret keys "Recent Advances and Innovations in Engineering (ICRAIE), 9-11 May 2014
[13] Islam, M.R. Siddiqa, A. ; Uddin, M.P. ; Mandal, A.K. ; Hossain, M.D. "An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography" Informatics, Electronics & Vision (ICIEV), 2014 International Conference 23-24 May 2014.

Author Profile

Latika is currently in M-Tech Final year in Computer Science and Engineering from PIET College, Haryana. She has published four Research Papers in international journals. Her research areas Include steganography, cryptography, and network security.