Society for Multidisciplinary & Advanced Research Techniques (SMART)
Trinity University, Lagos, Nigeria
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Harmarth Global Educational Services
ICT University Foundations USA
IEEE Computer Society Nigeria Chapter

33rd ECOWAS iSTEAMS ETech Multidisciplinary Conference (ECOWAS-ETech)

Encryption of Text in Image Over a Network

Stephen Hasford
School of Technology
Ghana Institute of Management & Public Administration
GreenHills, Accra, Ghana
E-mail: stephen.hasford@st.gimpa.edu.gh

ABSTRACT

Several recent attacks have arisen during electronic information transmission between a sender and a recipient over an unencrypted network. This has made threat actors eavesdrop and capture sensitive information being transmitted over the network since the information is in cleartext. Introducing an encryption protocol will protect data in transition from being eavesdropped on by threat actors, but only the recipient will be able to decipher and read the information. This term paper demonstrates a method of encrypting plaintext information data into an image to be sent over a network to the intended recipient.

Keywords: Encryption, Network, Image steganography

Proceedings Citation Format
Stephen Hasford (2022): Encryption of Text in Image Over a Network. Proceedings of the 33rd ECOWAS iSTEAMS Emerging Technologies, Scientific, Business, Social Innovations & Cyber Space Ecosystem Multidisciplinary Conference. University of Ghana/Academic City University College, Ghana. 29th Sept – 1st Oct, 2022.
Pp 184-188. www.isteams.net/ghanabespoke2022. dx.doi.org/10.22624/AIMS-/ECOWASETECH2022P36

INTRODUCTION

Threat actors can capture or eavesdrop on information transmitted over a network which is sent in plaintext and is not encrypted. This attack is called a man-in-the-middle attack when the threat actors intercept the information; they are sold on the dark web or used to attack the sender. It is important to add an additional layer of security using steganography or cryptography techniques. These techniques are used to hide information data in digital media. According to Amin et al. (2003), steganography hides the existence of the message from others while cryptography scrambles the message so you know it is there but cannot access it without a key. Cryptography and steganography are well-known and widely used techniques that manipulate information to hide its existence. Cryptography scrambles a message so it cannot be understood. It involves converting a message into an unreadable cipher. Abikoye et al. (2012) state A large number of cryptography algorithms have been created to date with the primary objective of converting information into unreadable ciphers.

2. LITERATURE REVIEW

Kapur and Baregar (2013) developed security using image processing to increase the security of transmitted data on the internet to a much-needed higher level by using the AES algorithm to encrypt the text message and embed it in a part of the image, thus making the text message challenging to find. Due to the rise in cybercrime activities over a network, implementing only network security won't be sufficient, but adding the image steganography technique will benefit transmitting confidential information.

The design of encryption of text in the image over a network

The Design of Steganography and Cryptography for Sending Pictures over a Network is in three phases; firstly, the message from the sender is encrypted using the blowfish algorithm. Next, the encrypted message is hidden inside the picture using the least significant bit algorithm, and lastly, the picture is sent over the network to the recipient. Below is the figure of the System architecture.

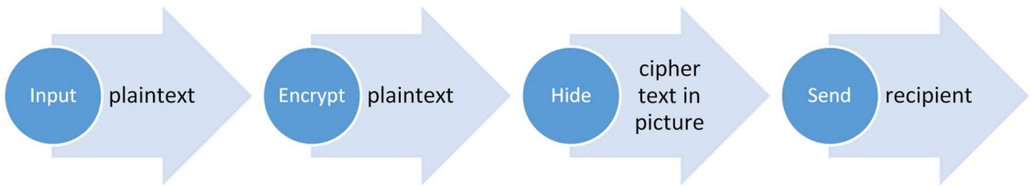

Figure 1: System Architecture

Steps for the encryption and decryption of text in image to be sent over a network

The process of hiding data inside a digital image using steganography and cryptography method is as follows:

For the encryption method

1. Upload a cover image where a secret message or a secret file will be hidden in.
2. The cover image can be any of the following filetypes (max file size = 300 KB): .bmp, .gif, .jpeg, .jpg, .png.
3. Also, less information hidden inside the cover image is better.
4. Enter a secret message or instead upload a secret file.
5. The secret message or secret file will be embedded inside the cover image.
6. The maximum size of the secret message is 5000 characters.
7. The secret file can be any filetype (max file size = 100 KB).
8. Enter a password for additional security.
9. If a password is entered, the same password is required to unhide the secret message or secret file from the cover image.
10. To prevent automated submissions an Access Code has been implemented for this tool. Please enter the Access Code as displayed above
11. Press the "Encrypt" button.
12. An encrypted image is created where the secret message or secret file is hidden inside.
13. Download encrypted image or secret file

For the decryption method

1. Upload an encrypted image where the secret message or the secret file is hidden inside.
2. If a password is specified during the encryption process, the same password is required here.
3. To prevent automated submissions an Access Code has been implemented for this tool. Please enter the Access Code as displayed above
4. Press the "Decrypt" button.
5. If a secret message is found it will be displayed in the text area.
   If a secret file is found it can be downloaded.

Below demonstrates how the process is done using the designed Steganography and Cryptography tool

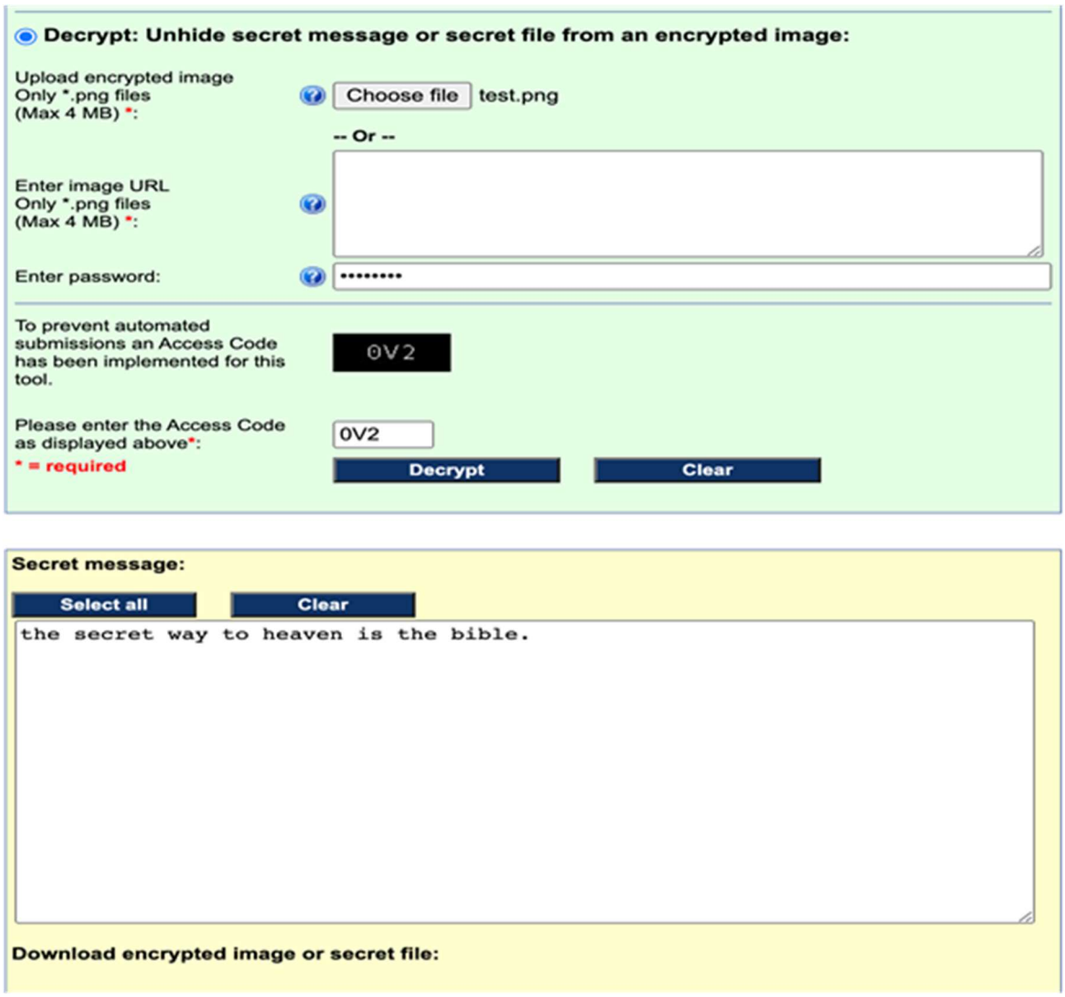

Figure 2: Encryption

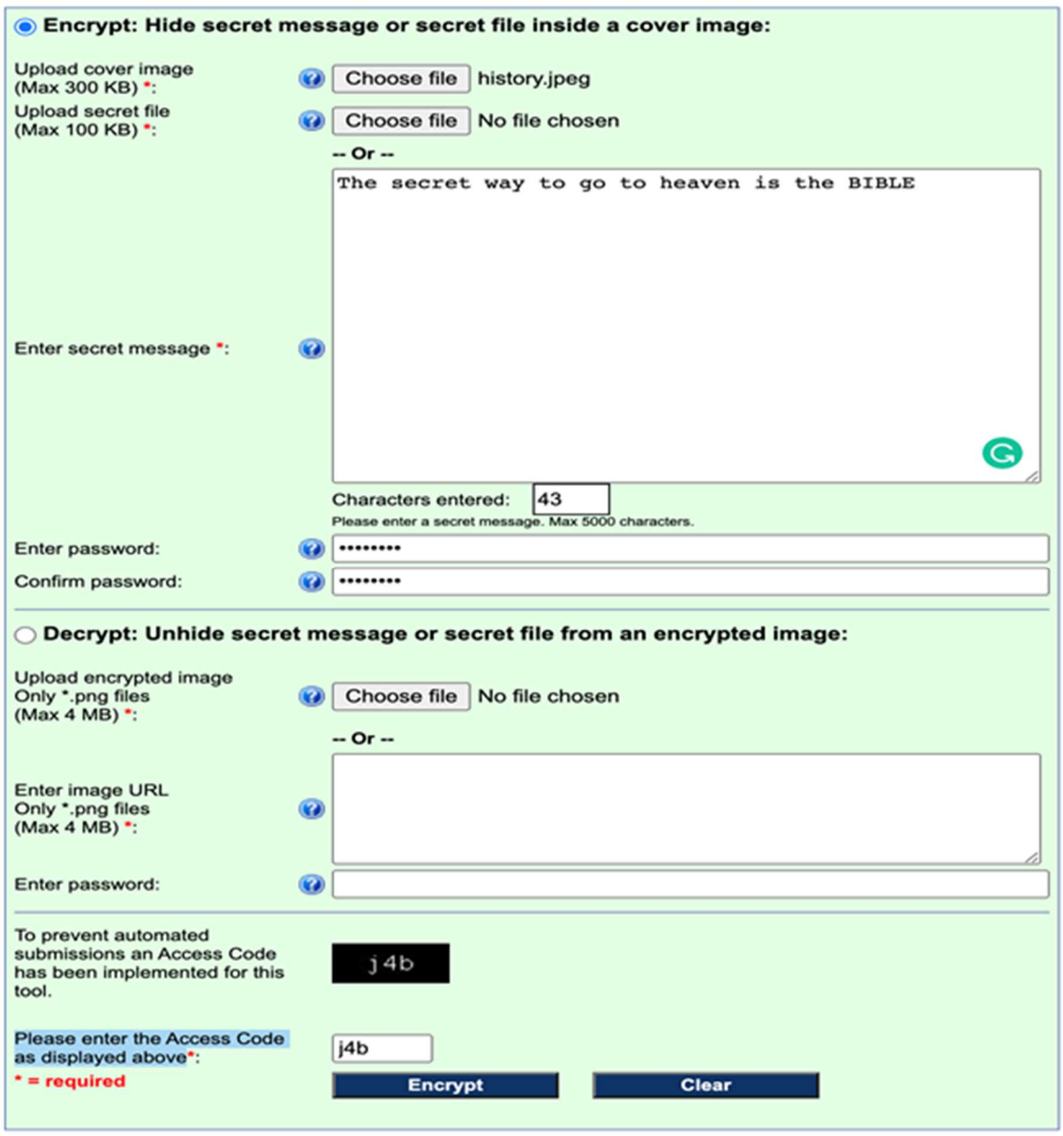

Figure 3: Decryption

Figure 4: Image to hide text

3. CONCLUSION

In this research, the text can hide inside an image transmitted from sender to recipient over a network using encryption (blowfish).
It is recommended that other formats of data source should be included, such as PDF, word documents, audio or wave file.

References

1. Kapur, J., & Baregar, J. A. (2013). Security using image processing. International Journal of Managing Information Technology (IJMIT), 5(2). https://www.researchgate.net/publication/276199119_Security_Using_Image_Processing
2. Amin, M. M., Salleh, M., Ibrahim, S., Katmin, M. R., & Shamsuddin, M. (2003). Information hiding using steganography, 21-25. https://www.researchgate.net/publication/4008787_Information_hiding_using_steganography
3. Abikoye, O. C., Adewole, K. S., & Oladipupo, A. J. (2012). Efficient Data Hiding System using Cryptography and Steganography. International Journal of Applied Information Systems (IJAIS), 4(11). https://www.researchgate.net/publication/277414511_Efficient_Data_Hiding_System_using_Cryptography_and_Steganography