ISSN 2278-3091

Volume 9, No.4, July – August 2020

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse261942020.pdf

https://doi.org/10.30534/ijatcse/2020/261942020

Securing Hidden Message Communication in Social Media using Stenography

Dr.A.Shanthini[1], Dr.M.B. Mukesh Krishnan[2]

[1]Associate Professor, Department of Information Technology, SRM IST,
Kattankulathur, Chennai 603 203, India, shanthia@srmist.edu.in

[2]Associate Professor, Department of Information Technology, SRM IST,
Kattankulathur, Chennai 603 203, India, mukeshkm@srmist.edu.in

ABSTRACT

Internet is a vital factor for information technology and communication for secured information. From the evolution of internet, providing security to information that are transmitted between nodes in network has become one of the most important aspect in networking. As millennials have made abundantly clear, social networks are often worn as an outlet for straight forward texts, used as an outlet for sending sensitive information without getting much attention from people around. Users don't comprehend their susceptibility. Social media offer a means to chat, share photos and uphold causes. They underestimate personage presence and significance to outsiders. So, a thing turns sloppy. All the personal contact details are very easily accessed by the hackers. Similarly, all of the browsing history, shopping record or other services are also hacked by the hackers with the help of social media connection.

In order to prevent this from happening, this paper aims to provide a technique to hide the necessary information. The technique used is AES encryption to encrypt text files and LSB Stenography technique to hide these encrypted text files in the images. Images are trendy wrap stuff worn intended for Stenography. In the sphere of digital imagery, many unlike image file formats, exist, for specific applications.

Key words : Stenography, Security, Algorithm, Social Network.

1. INTRODUCTION

The technique of sending a hidden message inside the image without the knowledge of the receiver is known as stenography. The problem includes third party cannot identify the presence of the secret message or be able to access it. The present study uses a text file which has the secret memo. This communication encrypted by means of the AES algorithm. The nonentity text is then hidden in a plaster sleeve (image)without any distortions[1]. This embedded file can then be sent across any social media platform as a harmless looking image[9]. On the receiver side, the message file can be extracted and then decrypted from the cover file to get our original message.

This program uses the AES algorithm to perform the cryptography part and then the randomized LSB technique is used to implement image steganography[5,8]. This kind of program can be helpful for frequent users of social networking websites like WhatsApp, Instagram, and Facebook, especially for those who need to send sensitive information through such websites.

Almost all social networking sites provide the facility for sharing and uploading media[10]. People who use social media share their life moments and events via images and videos. Aside from sharing life moments, people may also choose to send sensitive information via this platform[2]. It is risky because many data thefts such as illegal editing and misuse of data by the third party can occur. Sensitive information may include personal details.

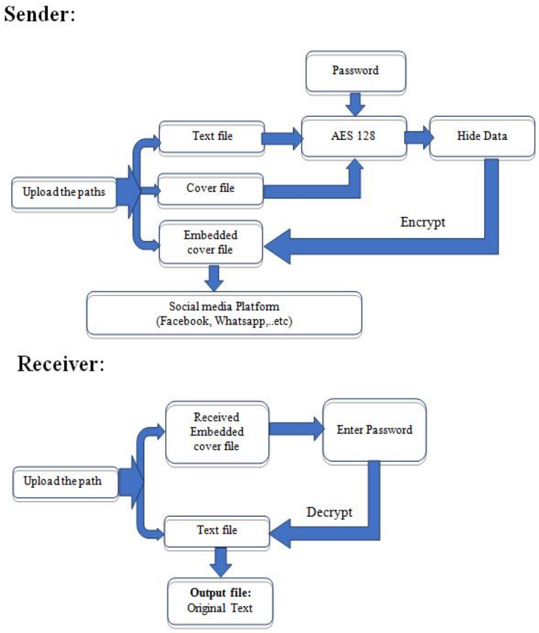
2. SECURING HIDDEN MESSAGE COMMUNICATION IN SOCIAL MEDIA USING STENOGRAPHY

The DES and its key size are too short for proper security. The 56–effective bits are brute forced pretty easily with the right resources. DES is applied 3 times to the information that are being encrypted[4]. The encryption key which is used for encryption is restricted to 56 bits. Since it is applied 3 times, the implementer can choose 3 discrete 56-bit keys or 3 identical keys. AES is used with a block length of 128 bits to carry out the block cipher process which is the most popular encryption algorithm with more mathematically formulated cryptographic algorithm with high efficiency[3,7]. The AES is allowed to choose various bit keys such as 128-bit key, 192-bit key or 256-bit key to enable it secure than 56 bit key of AES. AES uses permutation substitution method, which involves series of substitution and permutation steps to create encrypted block[6].

3. IMPLEMENTATION

The model to be built is implemented using the java code to check for errors. After building, the code is implemented. The output is in the form of a box that contains 2 options, either to hide data or to extract data. To hide data in the cover file the following steps are to be implemented:

- Upload the path of the text file in the “message file” dialogue box
- Upload the path of the cover file in the “cover file” dialogue box.
- Upload the path of the embedded cover file in the “Output stego file” dialogue box.
- Choose AES 128 as the encryption algorithm.
- Set a strong password which cannot be easily guessed by the brute force method.
- Click on the “hide data” option.
- Upload the “cover file”
- Skipped 0 file(s)” appears which depicts that the message has been successfully hidden inside the desired the cover file.


Sender:

Receiver:

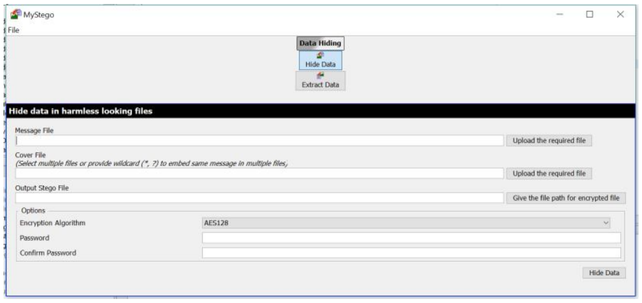
Figure 1: Block diagram- Sender and receiver

Once, this is done, the encrypted image is sent onto a social media platform like Facebook messenger, WhatsApp to the intended receiver where the cover file is to be decrypted. extract data from the cover file the following steps are to be implemented

- Upload the path of the received embedded cover file in the “Input stego file”.
- Upload the output file (which contains initially sent hidden message in the cover file) in the “Output folder for message file” dialogue box.
- Enter the password that was set by the sender.
- Click on the “extract data” option.
- A dialogue box which says “Message file successfully extracted from the cover file:” appears which depicts that the message has been successfully extracted from the received the cover file.

4. RESULT AND ANALYSIS

Figure 2 shows the hide data GUI which has the three dialog box paths of upload file, cover file, and output storage file it has an option of AES files 128, 192 or 256 and secured using the user authentication with user ID and password. Figure 3 shows the Extract data GUI three dialog to get input file and output file.



Hide data in harmless looking files

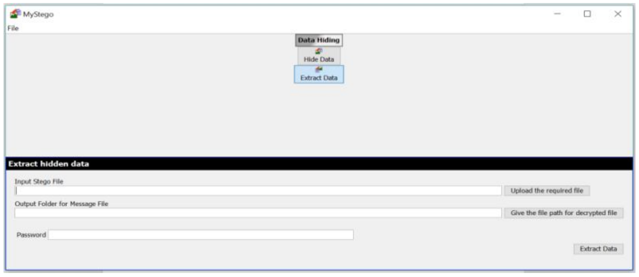
Message File

Cover File
(Select multiple files or provide wildcard (, ?) to embed same message in multiple files,*

Output Stego File

Options
Encryption Algorithm AES128
Password
Confirm Password

Figure 2: Hide data GUI



Extract hidden data

Input Stego File

Output Folder for Message File

Password

Figure 3: Extract data GUI

This system provides an easy and fast in transferring hidden messages, has a less failure rate and does not wait for busy servers and it is highly protected by providing a password

The embedded file can also be sent across social media and be safely decrypted to get the secret message. This means that as long as the receiver has the same project and the correct password, messages can be sent to any part of the world. Hence this helps solve the real-life scenario of protecting our privacy at any time even if an unauthorized third-party gains access to our social media account.

Table 1: Packet Delivery Ratio (PDR)

No. of. Transactions	Packet Delivery Ratio (PDR) (%)	
	DES	AES
50	91.28	95.34
100	86.67	89.34
150	81.12	83.42
200	75.21	78.39

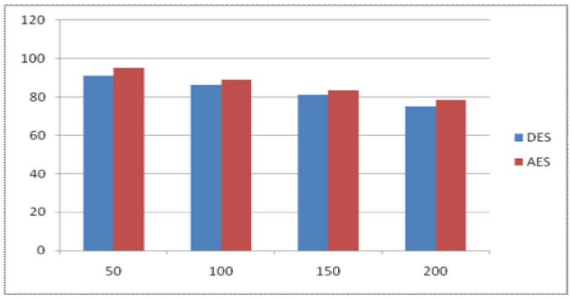


Figure 4: Packet Delivery Ratios (PDR)

Table 2: End to End interference

No. of. Transactions	**End-to-End interference (second)**	
	DES	**AES**
50	4.38	2.44
100	7.77	5.48
150	9.22	7.32
200	16.31	13.49

The system is tested with number of transaction for the performance parameters. The above given table1 shows average packet delay in percentage for various numbers of transactions such as 50, 100, 150 and 200. Similarly, table 2 shows end to end interference for the transactions. Figure 4 and figure 5 shows the graph of the same and the result shows under AES the system works better compared to the DES. LSB Stenography technique to hide these encrypted text files in the images with AES will be a secured and effective method for hidden transmissions.

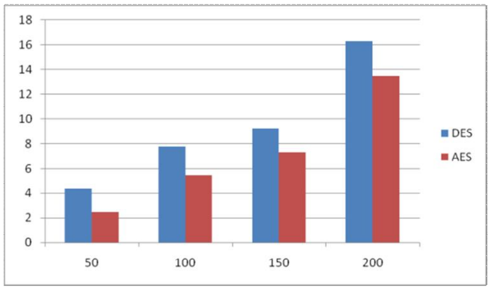


Figure 5: End- to- End interference

5. CONCLUSION

The effective method for securing hidden message communication in social media using stenography is proposed in this paper. The method was tested with the designing of a GUI based model and further the efficiency was tested by comparing the AES and DES with the packet delivery ratio and an end to end delay. LSB Stenography technique to hide these encrypted text files in the images with AES will be a secured and effective method for hidden transmissions.

REFERENCES

1. J. Kodovsky, J. Fridrich, and V. Holub. **"Ensemble classifiers for steganalysis of digital media".** IEEE Transactions on Information Forensics and Security, 2012. https://doi.org/10.1109/TIFS.2011.2175919
2. T. Pevny and J. Fridrich. **"Merging Markov and DCT features for multiclass JPEG steganalysis. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents",** 2007.
3. SalehSaraireh **"A Secure Data Communication System Using Cryptography and Steganography"** International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.3, May 2013. https://doi.org/10.5121/ijcnc.2013.5310
4. Geetha Vani.B, Prasad. E.V. **"Scalable And Highly Secured Image Steganography Based On Hopfield Chaotic Neural Network and Wavelet Transforms"** IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 3, No 1, ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784, May 2013
5. Vijay Kumar Sharma, Vishal Shrivastava **"Steganography Algorithm for Hiding Image in Image by Improved LSB Substitution by Minimize Detection"** Journal of Theoretical and Applied Information Technology, Vol. 36 No.1, and ISSN: 1992-8645, E-ISSN: 1817-3195.15th February 2012.
6. Ugala.K, Venkata Rao K **"Steganography"** International Journal of Engineering Trends and Technology (IJETT) – Vol. 4, issue 5, May 2013.
7. VikasTyagi, Atul Kumar, Roshan Patel, Sachin Tyagi, Saurabh Singh Gangwar **"Image Steganography Using Least Significant Bit With Cryptography",** Journal of Global Research in Computer Science(JGRCS) Vol. 3, No. 3, ISSN-2229-371X, March 2012.
8. Hajduk V , Broda V , Kováþ O and Levický D, **"Image steganography with using QR code and cryptography,"** 26th Conference Radioelektronika, IEEE pp. 978-1- 5090-1674-7, 2016
9. A. Gaikwad and K.R.Singh, **"Information Hiding using Image Embedding in QR Codes for Color Images: A Review,"** International Journal of Computer Science and Information Technologies, Vol. 6 (1) , 2015
10. G, Vadivu, Fancy, C. Sivasankari, S. Sornalskshmi, K..**"Shortest Path of a Graph using Centrality Measures",** International Journal of Advanced Trends in Computer Science and Engineering. Vol.9., 3898-3903, 2020 https://doi.org/10.30534/ijatcse/2020/210932020