IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.8, Issue.7, July 2020 E-ISSN: 2347-2693

Image Steganography And Cryptography Using Three Level Password Security

Jeena Thomas[1*], Jeena M. Roy[2], Malu M.[3], Vrinda Vijayan[4], Anoop S.[5]

[1,2,3,4,5]Dept. of Computer Science and Engineering, St Thomas College of Engineering and Technology, APJ Abdul Kalam Technological University, Kerala, India

[*]*Corresponding Author:jeenathomas1998@gmail.com*

DOI: https://doi.org/10.26438/ijcse/v8i7.3235 | Available online at: www.ijcseonline.org

Received: 06/July/2020, Accepted: 16/July/2020, Published: 31/July/2020

***Abstract*—** Cryptography and Steganography are two favourite techniques used by developers for security reasons.Cryptography is the study of information hiding and verification. It includes the protocols,algorithms and strategies to securely and consistently prevent or delay unauthorized access to sensitive information and enable verifiability of every component in a communicate.Steganography is the process of hiding text in an image**.**we propose an encrypting system which combines techniques of cryptography and steganography with data hiding which is highly useful in secret keeping areas. Image steganography and cryptography using three level security is used for transferring text message from sender to receiver.The main aim of project is to provide the user a secure way that helps the user to send and receive secret messages.There is three level authentication system that validates user for accessing the system only they have input correct one time password.The project involves three levels of authentications for the sender and receiver. In this sender will have to first go through all the three stages of authentication.After going through all the stages the senders text will be encrypted using the cryptography algorithm.These encrypted text will be hidden inside the image.After getting this image he can be send this image and verify OTP to receiver's mobile number.The receiver also has to through all the stages of authentication and use one time password for verification and decrypt the image and get the message hidden inside the image.

***Keywords*—**Cryptography,Steganography,Security,OTP(OneTimePassword)

I. INTRODUCTION

Security of information is one of the major issue facing in today's world. As we all know that the security of information plays a major role for sharing confidential data between two parties. Cryptography and Steganography are the two techniques used for sharing the confidential data. cryptography is used for converting plain text (human readable text) to cipher text (encrypted text).steganography is used for hiding this text inside an image. To overcome the drawback of the existing system, we use three level authentication system with two different algorithms helps to protect the data from unauthorized user. An OTP generates in receiver side should be confidential. The receiver can verify the OTP and decrypt the message,it makes the message highly confidential.

The contribution of this work is as follows:

1. A three level authentication system with two different algorithm and OTP used for securing highly confidential data.
2. First level authentication is to encrypt the data using AES algorithm and Second level authentication is to encrypt again the data using SHA256 algorithm
3. Third level authentication is using One Time Password for decrypting the message.
4. The work carries out in-depth studies in cryptography and steganography techniques.
5. The main objective is to study how secure the confidential data with AES and SHA256 algorithm.

II. RELATED WORK

S Usha,G A Sathish Kumar & K Boopathybagan proposed "A Secure Triple Level Encryption Method Using Cryptography" which is an encrypting system.This technique combines the feature of cryptography and steganography with same algorithm.In this paper, use two levels of data encryption. After the data encryption is done, the cipher text is hidden inside the image using steganographic techniques. Asymmetric key cryptography is the technique where two keys are used. One key is used to lock or encrypt the plain text, and another to unlock or decrypt the cipher text. Neither key can do both the functions. One of these key is published or made public and the other is kept private. This technique has comparatively slower data rate throughputs than the symmetric key technique.Symmetric key cryptography is actually the technique by which identical cryptographic keys are used for the purpose of both encryption and decryption. The receiver can get back original data by using the key. The symmetric key cryptography provides

high data rates, usage as primitives to construct various cryptographic mechanisms and can be combined to produce stronger ciphers. The main fact here is that the security of data depends on the security of the key. So, care should be taken while exchanging keys between the sender and the receiver.

III. METHODOLOGY

A. PROPOSED SYSTEM

Working of the proposed system can be explained as below:

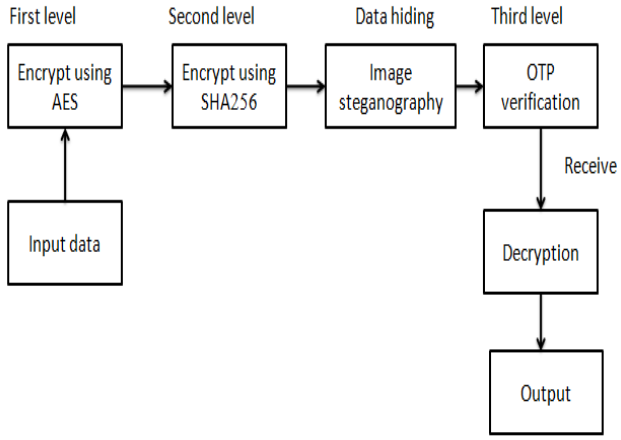

Fig 1: Functional block diagram of proposed system

In the given block diagram initially the text data is given to the system. At first the text data is encrypted using the Advanced Encryption Algorithm(AES),which is symmetric block cipher and has 128 bit symmetric key.After this encryption, text data is again encrypted using Secure Hash Algorithm(SHA256), which has 256 bit hash code and symmetric key.Here the two level authentication completed.Then hiding the encrypted data in an image which is steganography.Then receiver can decrypt the message using One Time Password(OTP) received in receivers phone number which is already given in registration process.After entering the OTP,the decrypted message will be popuped on the screen.The sender and receiver has username and password for entering their own profile.

B. SYSTEM REQUIREMENTS

a) HARDWARE REQUIREMENTS

- Processor (min i3)
- Hard Disk (min 160GB)
- RAM(min 2GB)

b) SOFTWARE REQUIREMENTS

- OS-Window/Linux
- Html Css Java Script
- Php
- MY SQL
- Visual Studio
- XAMPP

IV. RESULTS AND DISCUSSION

For complete investigation of the proposed system considers the following aspects:

- Security: The studies evaluates the secure ways of transferring the confidential data among two parties.
- Efficiency: The studies evaluate the efficiency of the system by comparing the existing system.

The proposed system shows how the secret message passing from sender to receiver. It is very useful in highly confidential areas like military etc….

There are two categories for performing the process:

1. Sender: sender can create their own profile by using username and password. Then choose image from the file and set the secret message then send to receiver
2. Receiver: receiver can also create their own profile by using username and password. Then click receive data and decode the secret message hidden in an image by verifying the OTP received in his mobile number.

The final output shown in the figures below:

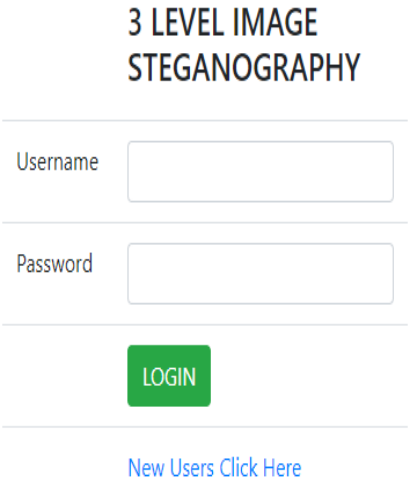

Fig 2: first interface of 3level

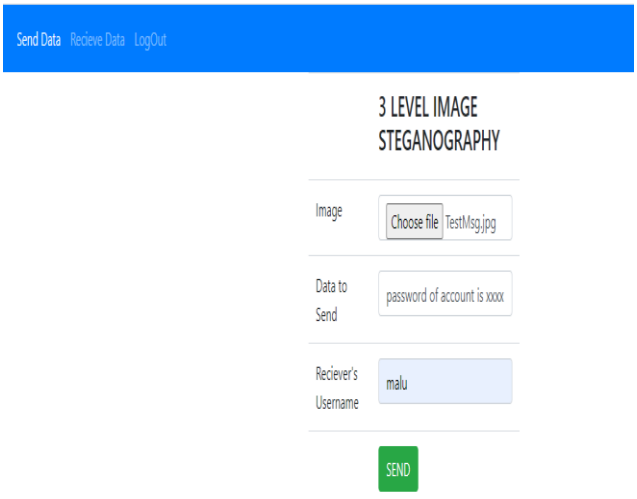

Fig 3: sender's profile

Fig 4: receiver's profile

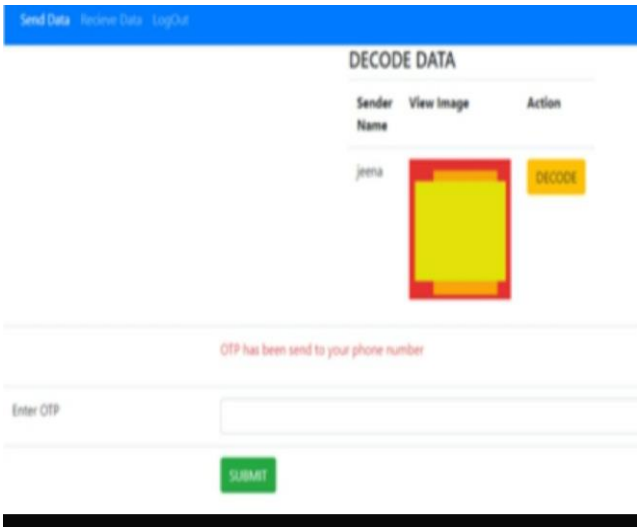

Fig 5: Enter OTP and SUBMIT

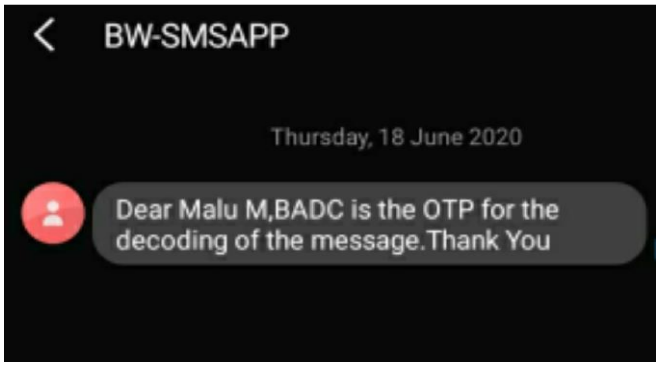

Fig 6: receiver receives an OTP

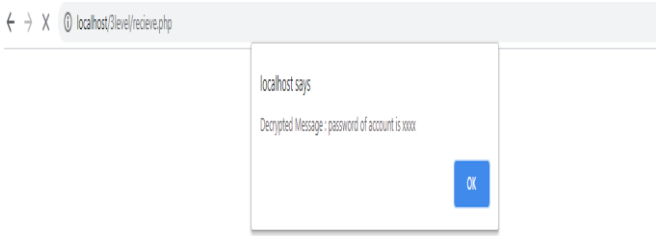

Fig 7: Decrypted message popuped on screen

V. CONCLUSION AND FUTURE SCOPE

This is a system for passing confidential data among two parties. The system mainly looking for security. It provide high security and confidentiality among the authorised user. Authorised users can transform their own secret data through this three level authentication system. There are three levels of authentication that must provide the data highly protected and prevent the accessing of unauthorised user. Two different algorithms for encryption make the secret data become secure. Our application with its complete analysis is a significant improvement on current cryptography and steganography tools.

A. ADVANTAGE AND LIMITATIONS

a) ADVANTAGES

- Highly helpful in military purposes and other secret keeping areas
- Combination of cryptography and steganography provide high security
- Face-to-face conversation.
- Continuous attention to technical excellence and good design.
- Regular adaptation to changing circumstances.

b) LIMITATIONS

- Image must be in the form of .jpeg or .png format.
- The proposed system cannot work efficiently if the hardware and software requirements are not met correctly.
- Proper network should be available for uninterrupted service.

B. FUTURE SCOPE

The future scope of our proposed system is that can transfer the audio and video messages among the authorised users. Now it is only applicable for text data.

VI. ACKNOWLEDGMENT

This paper has been supported by Department of Computer Science Engineering, St.Thomas college of Engineering and Technology and authors would like to thank our guide Asst.Prof.AnoopS,Dept. Of ComputerScience Engineering, St.Thomas college of Engineering and Technology,Kerala.

REFERENCES

[1] Rupesh Gupta , Dr .Tanu Preet Singh"New Proposed Practice for Secure Image Combing Cryptography Steganography and Watermarking based on Various Parameters" 2014 International Conference on Contemporary Computing and Informatics (IC3I).

[2] Mamta Juneja, Parvinder Singh Sandhu"Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption"2009 International Conference on Advances in Recent Technologies in Communication and Computing.

[3] International Journal of Applied Information Systems "Efficient Data Hiding System using Cryptographyand Steganography".

[4] ICTACT JOURNAL ON IMAGE AND VIDEO PROCESSING, FEBRUARY 2015 "Pixel pattern based steganography on images".
[5] S.Lyu and H. Farid, "Steganography using higher order image statistics, "IEEE Trans. Inf. Forens. Secure,2006.
[6] "Advanced Encryption Standard "(AES), National Institute of Standards and Technology (NIST), U.S. FIPS PUB 197 (FIPS 197), 2001
[7] T.Morke1, "An Overview of Image Steganography", Department of Computer Science, University of Pretoria, South Africa
[8] Piyush Marwaha, Paresh Marwaha,"Visual Cryptographic Steganography in Images", Infosys Technologies Limited, India
[9] William Stallings, "Cryptography and Network Security: Principles and Practices", Third edition, Chapter 2 and Chapter 5.
[10] James Lyons 'The Playfair Cipher.". Practical Cryptography I, July 2009.
[11] Swati Nimje, Amruta Belkhede, Gaurav Chaudhari, Akanksha Pawar and Kunali Kharbikar,"Hiding Existence of Communication Using Image Steganography " in International Journal of Computer Science and Engine and Engineering(IJCSE), Volume-2, Issue-3 ,E-ISSN: 2347-2693.Mar-2014.
[12] Unik Lokhande, A.K.Gulve Steganography using Cryptography and Pseudo Random Numbers • in an International Journal of Computer Applications (0975 " 8887) Volume 96" No.19, June 2014 .
[13] M. S. Sutaone,M.V. Khandare,"Image Based Steganography Using LSB Insertion Technique" in 2008 IET International Conference on Wireless, Mobile and Multimedia Networks.
[14] Arati Appaso Pujari,Sunita Sunil Shinde,"Data Security using Cryptography and Steganography" in IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 4, Ver. V (Jul.-Aug. 2016), PP 130-139.
[15] Pooja Rani, Mrs. Preeti Sharma,"Cryptography Using Image Steganography" in an International Journal of Computer Science and Mobile Computing, Vol.5 Issue.7, July- 2016, pg. 451-456.
[16] Miftah Ul Uroos, Sukhvinder Kaur ,Muheet Ahmed Butt , Steganography: A Comparative Survey Conducted on Digital Images • in IOSR Journal of Engineering (IOSRJEN) ISSN (e): 2250-3021, ISSN (p): 2278-8719 Vol. 08, Issue 10 (October. 2018), ||V (I) || PP 52-61 .

AUTHORS PROFILE

Ms. Jeena Thomas a dedicated and compassionate professional who is currently pursuing her Bachelor's degree in Computer Science and Engineering at St. Thomas College of Engineering & Technology, Kerala, India under APJ Abdul Kalam Technological University. She posses strong interpersonal skills, demonstrating the utmost discretion and integrity when dealing with confidential information.She is a member of IEEE.Her main research work focuses on Network security.

Ms. Jeena M Roy a dedicated and compassionate professional who is currently pursuing her Bachelor's degree in Computer Science and Engineering at St. Thomas College of Engineering & Technology, Kerala, India under APJ Abdul Kalam Technological University. She is a member of IEEE.She is having interests in Software testing and is currently reasearching in this area.

Ms. Malu M a dedicated and compassionate professional who is currently pursuing her Bachelor's degree in Computer Science and Engineering at St. Thomas College of Engineering & Technology, Kerala, India under APJ Abdul Kalam Technological University. She is very talented and hardworking.She is having interests in web development and is currently reasearching in this area.

Ms. Vrinda Vijayan a dedicated and compassionate professional who is currently pursuing her Bachelor's degree in Computer Science and Engineering at St. Thomas College of Engineering & Technology, Kerala, India under APJ Abdul Kalam Technological University. She is excellent in working with others.She is having interests in networking and is currently reasearching in this area.

Mr. Anoop S pursued Bachelor of Technology in Computer Science and Engineering from MG University, Kottayam and Master of Engineering in Computer Science and Engineering from Anna University, Chennai. He is currently working as Assistant Professor in the Department of Computer Science and Engineering, St. Thomas College of Engineering & Technology, Kerala, India. He is a member of Computer Society of India (CSI). He has published three papers in reputed International journals and conferences. He has 7 years of teaching experience. His interested areas are cryptography and Network Security.

