Image Steganography over Crypted Text using Two Factor Verification

Basamma* and P. S. Shilpashree**
*-**Department of Electronics and Communication, Siddaganga Institute of Technology, Tumakuru, Karnataka-572103
*basammal@gmail.com
** shilpa.sit@gmail.com

Abstract: Nowadays digital communication plays a very essential role in our daily life, because lots of applications and online activities are based on internet. Transferring the secure data over the network has become a major issue. Protecting the confidentiality and information integrity against unauthorized user to access and use is very important. Today many systems are available with various effort to maintain the secure data and to overcome these issues. Cryptography and steganography are the two important methods available for the secure message. This paper proposed a dynamic password generation approach for authentication measure. Once the user register to the system the identification code will be sent to the registered Email ID of the user. Later, user will input it as PIN to access the confidential data. This paper also contains the strength of combined cryptography and steganography techniques to enhance the security of communication over an open channel.

Keywords: Advanced encryption algorithm(AES), Cryptography, Least Significant Bit(LSB), Steganography.

Introduction

The security and integrity of data is the main concern in today's situation due to ever increasing social media and online activities. There are certain individuals and groups which are doing the improper acts by registering the fake account. This obviously gives the bad name to the social media owners and online sites. Therefore, preventive actions are very necessary to reduce these activities. One way to improve the security in registration process is by producing the authentication code to activate and verify the user account. Two factor authentication method is one way to alleviate users is main concern. One of the strong authentication method is dynamic password generation, which changes with the dynamic factors like timestamp. The dynamic password is anti-theft because of its only one-time usability and randomization. Only legitimate users should be able to access information and use. The activation message contains activation key sent through SMS to the email or mobile phone numbers to ensure the correct account. Cryptography is a science which involves an encryption and decryption pair. These are the two major techniques to prevent an unauthorized person to access into network. Cryptography technique is not only used for secure communication it can also be used for authentication purpose. Nowadays, present information is in the form of message, images, videos including sending information in the form of file which is very complicated. There are several forms of attacks on data and information such as hackers and crackers.

To overcome these problems cryptography and steganography are used. Cryptography converts original information (plain text) into unreadable format (Cipher text) [1]; where as steganography is an art of hiding the secrete message in a protection media so that the existence of the message cannot be known to others. It is mainly used in military, diplomatic applications. Steganography is different from Cryptography it does not attempt to hide the existing message. It provides a high level of safety to the information but it does not provide solution for data integrity, authentication etc. However, it is difficult to find specific algorithm that covers various factor such as security, data integrity, authentication and complexity. Crypto-Steganography techniques overawed each other's weakness and makes hard for the hackers to attack or steal sensitive data.

There are many methods available for secure transmission, one of them is least significant bit (LSB) in which the message is encoded using the Advanced encryption standard algorithm(AES). The main aim is to improve the steganography data strength by incorporating the cryptography to encrypt the secret message.

Literature Review

Authentication

Authentication is a use of one or more mechanism to confirm that correct user should authenticate the system [2]. It is used to access a login account, accessing different kinds of services which are carried out by alpha-numeric password. The alternative authentications are in the form of biometric which includes finger print, iris and heartbeat. Limitation in the biometric authentication leads to development of validation of authentication method. Also, the biometric-based authentication is comparatively luxurious and raises secrecy concern.

Cryptography

Cryptography is the Greek word, crypto means confidential and graphein means writing. The process of altering the data into unreadable format is called cryptography. Encryption, decryption, secret key, plain text and cipher text are the components of cryptography. There are three types of techniques available i.e. public key(asymmetric) cryptography, secret key(symmetric)cryptography and hybrid cryptography.

- *Symmetric cryptography*

In this type of cryptography system sender and receiver uses an identical key to encrypt and decrypt the data. It is also named as a secrete key cryptography. The key sharing has made before the communication starts. The secrete key plays a very important role in this system. Example, DES, 3-DES and AES.

- *Asymmetric cryptography*

In this type of cryptography system sender and receiver uses different key to encrypt and decrypt the data. In Asymmetric key cryptography technique, a pair of keys are secret key and public key. One is used for encrypting the plain text, and the other is used for decrypting the cipher text. Example, RSA.

- *Hybrid cryptography*

It is a type of encryption that joins two or more encryption system. It is a combined symmetric and asymmetric encryption it takes the strengths of both the system. The strengths are speed and security respectively. Hybrid cryptography is considered as a highly-secured cryptography system.

Advanced Encryption Standard(AES) Algorithm

AES is a block cipher is an encryption standard. It uses a static block size of 256 bits as a plane text and produces a cipher text of same length. The key length can be of 128,192 and 256 bits therefore it is called as AES-128, AES-192 and AES-256. It has 10 rounds of substitution and permutation for AES-128 bit key,12 and 14 for AES-192 and AES-256 respectively. The encryption procedure is iterative in nature. Each iteration is recognized as rounds. For each round 256-bit input data and 256-bit key is required. Four words of key needed in one round. So, the input key must be expanded to the required number of words, which depends upon the number of rounds. The input of next stage is the output of present stage. In AES system, same secret key is used for both encryption and decryption. As it is symmetric cryptography the key transmitted before the communication starts. So, it provides easiness in design. Figure.1. shows the structure transformation of AES encryption process.

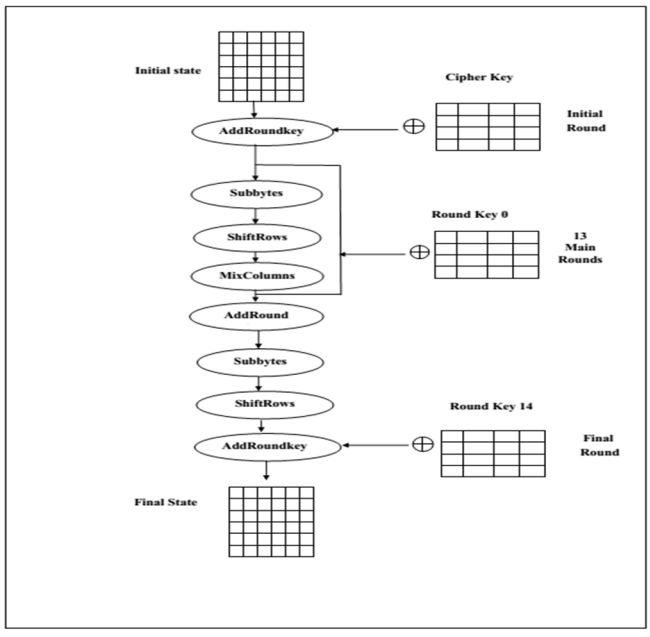

Figure.1. 256-bit AES encryption process

1.**AddRoundKey:** This is also called as an initial round. The initial state or plain text is XOR with the cipher key or keys in round-0.

2.Subbytes: Independently operates in each byte of the state every state is substituted with the input in table substitution box or s-box. This process gives the principle of non-linearity present in cipher.

3.Shiftrow: cyclically shifts the rows of the state over different offsets.
4.mixcolumns: it will do randomization of data in each column. This does not operate in the last round of algorithm.

Steganography

Steganography means covered writing. The main aim of steganography is to insert the secrete data in an image such a way that it will not be able to notice a secrete data existing in the image except sender and receiver. Steganography essentially uses a cover media which contains some redundant bits. This technique replaces these redundant bits of the media with that of the secret information. however, as this technique modifies the statistical property of the media, it stands behind detectable traces. There are various types of steganography which includes [3].

- *Image Steganography*

Image steganography is a technique of hiding the information within an image consequently there will not be any major changes in the original image. LSB embedding algorithm is one of the conventional image steganography algorithm.

- *Audio Steganography*

The method of hiding secret data behind any audio is known as audio steganography. There are many procedures available for hiding secrete data as LSB, phase coding etc...

- *Video Steganography*

The process of hiding secrete data in a video is known as video steganography. Video consist of audio as well as images hence, one can use both image and audio steganography for video steganography.

- *Text Steganography*

Text steganography is a process of hiding the secrete data in a text. Text steganography require smaller amount of memory as it can only store text.

Least Significant Bit(LSB)

Least significant bits is one of simple method for inserting information in cover image. The message is directly inserted into the least significant bit plane of the cover image in a deterministic sequence. Moderating the least significant bit does not result in human-perceptible change because there is small change in amplitude. One can use 8-bit or 24-bit image to hide the secrete message and 24 bit images are suitable for hiding huge amount of information. LSB is simple and suitable for hiding the secrete data [4].

For example, consider 3 pixels of a 24-bit color image, using 9 bytes of memory
(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100110 11101001)
The character A, which binary value equals 10000001, is inserted, the following grid results:
(00100111 1110100**0** 11001000)
(0010011**0** 11001000 1110100**0**)
(11001000 00100111 11101001)
In this case, the four bold bits are the bits that were modified. Since the letter A needs eight bytes to hide, the ninth byte can be used to hide the succeeding character of the secreted message.

Proposed Work

This paper proposes a system with two step of authentication which is important to add an additional level of safety to the transmitted data.

Authentication

The complete is composed of two steps:

- *User Registration*:

In this stage user registers himself on by giving cloud environment to his/her specifics like user first name, last name, Mobile number and the most important one is valid email id.

- *Authentication during log in: After the successful*

Registration process the user attempts to log in on the cloud environment. When he attempts to login the system asks user to give his/her user name as well as password. Only the pre-registered user can only be able to access the system. During registration process the dynamic code is sent to the user through SMS to the Email [5]. This procedure occurs every time user logins in into the system. The email account of user is considered as being safe on which secrete gen could be sent and only registered user has access to his account. This confirms privacy as well.

Image Steganography Authentication system is shown in Figure.2. (a). The first step is to fill all the details like user name, mobile number and Email ID of the user. Once the user submits the form One Time Password is sent to the Registered Email

ID. The next step is to verify the OTP. The user will enter the OTP, if the OTP is correct the password is generated and sent to the Email otherwise the system throws an error message like enter the correct OTP.

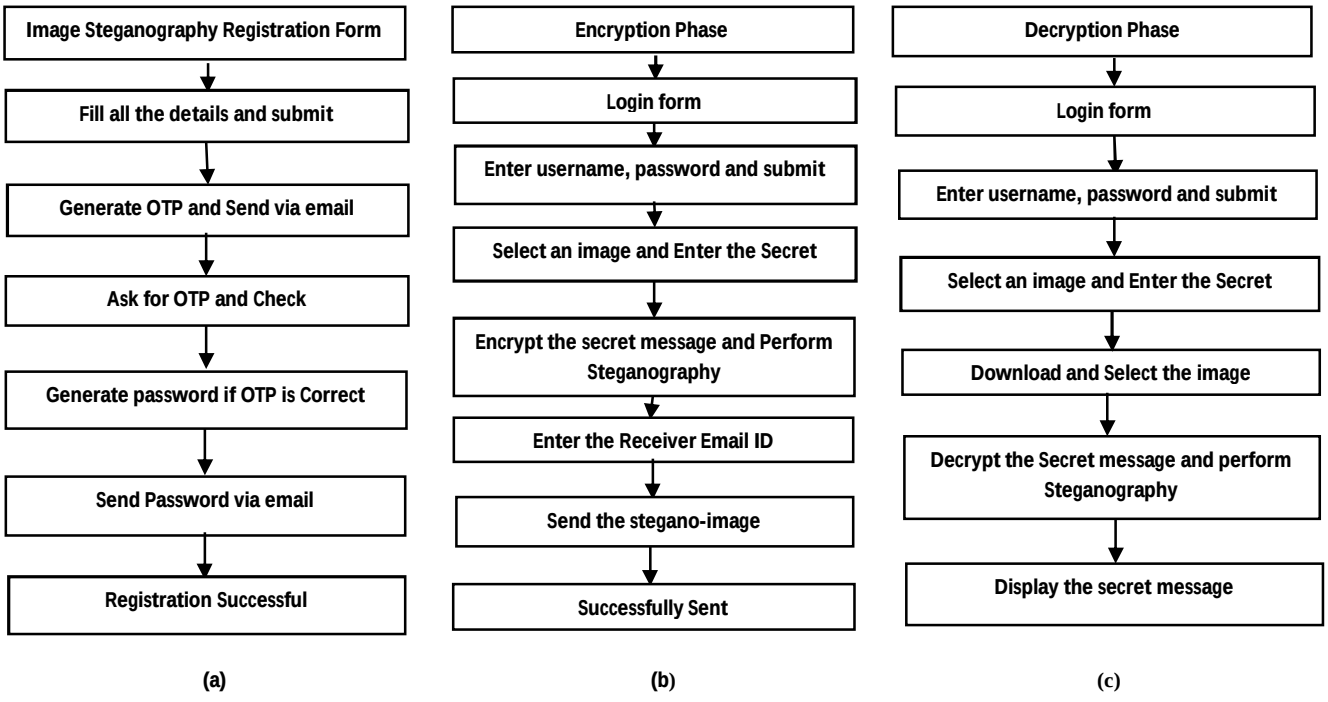

Figure.2. (a) Image Steganography Authentication System, (b) Encryption Process, (c) Decryption Process

Encryption

Encryption is used to hide the secret data in digital image. The figure.2. (b) shows the encryption process. In this Encryption phase, first step is to log into the system by entering user name and password. Only preregistered user can use this system. Select the image and enter the secret message. By using AES algorithm, the message is encrypted and given as an input to the Image Steganography. When user enters the Email id of the receiver the stegano-image is sent to the receiver

Decryption

To read the Secrete message from stegano-image the decryption algorithm is used. figure.2. (c) shows the Decryption process. Once the user enters the details he/she can perform decryption by downloading the Stegno-image from the Email ID. The Secret message is displayed.

Experimental Results

Experiment performed on 256*256 Lena color image. The proposed method achieves the extra security of the information very effectively by using two factor authentication method. To implement image steganography over crypted text it is very important to determine the length of the secret message to recover the secret message from the image. The message is crypted using Advanced Encryption Algorithm(AES) 256-bits. Encryption process and given as input to the image steganography. Information hiding in LSB of an image, the source image stored in a python Buffered Image. 256 bit key AES encryption is performed using python 3.4 cryptography libraries. The AES encrypted secret communication adds extra security to the proposed technique. The cryptography and steganography are combined to increase the strengths of the algorithms. The transmission characters have been converted to hexadecimal number it is possible that the same character represented in different code, and may be different character can be characterized in the same code. Along with this two-factor verification method also adds security and integrity. So, that only legitimate user can access the system and it is very difficult for others to hack the system. Simple, short and effective secrete key used to extract the secrete message. By using these techniques, we can achieve secure communication.

Steganography Registration form is shown in figure.3.(a) This is the first step of registration process where user enters all the details like user first name(Basamma), last name(L), mobile number (7353641212) and email id(basmmal@gmail.com). Once the user submit the form OTP is sent to the registered email id. OTP verification form is shown in figure.3.(b). This is the second step of registration process where the user enter the OTP received from the registered email. Registration

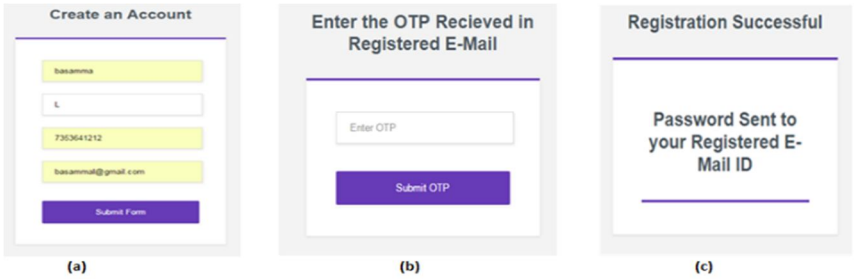

Figure.3. (a) Steganography Registration form, (b) OTP verification, (c)Registration Successful message after completion of registration process

Successful memo is shown in figure.3.(c). If the OTP is correct the password is sent to the registered email id otherwise it will show the 'Enter correct OTP' memo. This is the last step of registration.

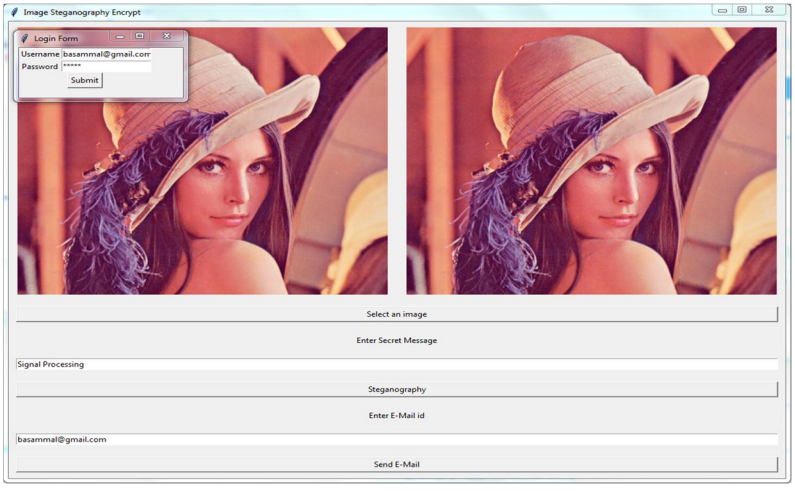

Figure.4. Image Steganography Encryption

Image Steganography encryption process is shown in figure.4. The user select an image and the text. The secret text is encrypted using AES algorithm and this encrypted text is given to the steganography. The stegano-image is sent to the receiver. Image steganography decryption process is shown in figure.5. The user download the stegano-image from the email id and perform AES decryption. The secret message is displayed.

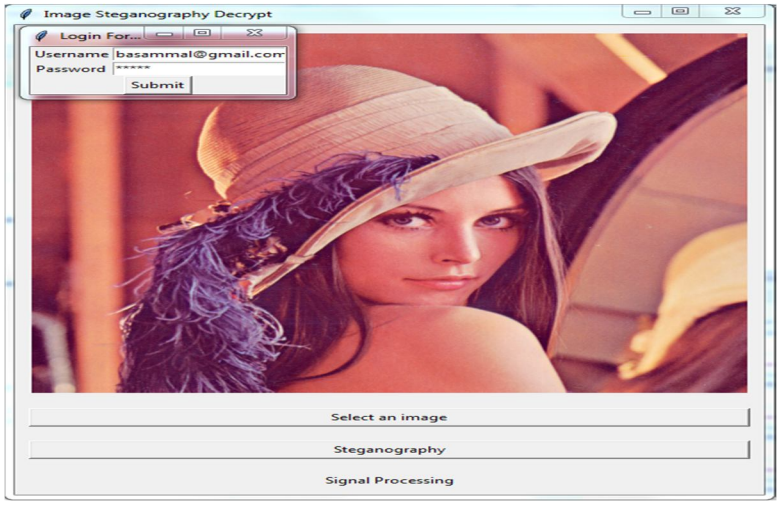

Fig.5 . Image Steganography Decryption

Conclusion

The proposed authentication and Crypto -Steganography techniques effectively enhances the security and the same is shown in the results. This method can also be applied to the Video, Audio and text along with different types of Cryptography algorithms.

References

[1] Shailesh Nana Kumavat, Pavan Patil, Ashwin Yeole and Yogesh Patil, "Highly Secure Steganography using Crossover Algorithm and Unbreakable Cryptosystem", International Journal of Sceintific Engineering and Technology Research, ISSN 2319-8885, Vol.04, Issue.08, April-2015, Pages:1499-1501.

[2] Namrata Thakur, Mrs.Vimmi Pandey, "An Approach of Authentication in Public Cloud using Two Step Verifictaion Code", International Journal of Emerging Research in Management & Technology, ISSN: 2278-9359 (Volume-2, Issue-5).

[3] Rina Mishra and Praveen Bhanodiya, "A Review on Steganography and Cryptography", 2015 International Conference on Advance in Computer Engineering and Applications(ICACEA), IMS Engineering College, Ghaziabad, India, IEEE 978-1-4673-6911, April 2015.

[4] Shikha Mohan and Satnam Singh, "Image Steganography:Classification, Application and Algorithms,", International Journal of Core Engineering & Management(IJCEM), Volume 1, Issue 10, January 2015.

[5] Kayigana Virgile and Huiqun Yu, "Securing Cloud Emails Using Two Factor Authentication Based on Password/Apps in Cloud Computing,", International Journal of Security and Its Applications, Vol. 9, No. 3 (2015), pp. 121-130.