HIDING ENCRYPTED TEXT USING TEXT AND IMAGE STEGANOGRAPHY: A DUAL STEGANOGRAPHIC TECHNIQUE

[1]PRITI SEHGAL, [2]SARVESH RAWAT, [3]SAURABH KAUSHIK, [4]SHAFAQ ALI, [5]ROHIT YADAV

[1]Associate Prof., [2345]B.Tech, Department of Computer Science, Keshav Mahavidyalaya, University of Delhi
E-mail: [1]psehgal25.08@gmail.com, [2]sarvesh.dav@gmail.com, [3]isaurabhkaushik@gmail.com

Abstract - Today, in this new era of internet, Information Security is becoming a biggest challenge for the world due to the rapid growth of internet users day by day. Unauthorized access to secret data can have serious repercussions like financial loss etc. One of the best techniques for secure communication is Steganography-or covert writing. It is an art of hiding the very existence of communicated message itself. In this paper we present a state of art dual steganographic technique. Dual Steganography combines two security mechanisms, steganography and cryptography both together. This mechanism has advantages of providing high security, low time complexity but this mechanism does not enhance capacity, robustness, and image quality. This paper proposes a new dual steganography technique with an additional level of security. The proposed algorithm embeds secret text message in cover image in three phases. The three phases include vigenere cipher technique, white space text steganography technique and LSB image steganography technique. Cover text containing encrypted data is hidden in an RGB image in RGBBGRRG order. Performance of proposed steganography technique has been evaluated by calculating values of MSE(Mean square error), PSNR(Peak signal to noise ratio).

Keywords - Steganography, Cryptography, Dual steganography, LSB, PSNR, MSE.

I. INTRODUCTION

Internet had eased the way of transferring data and communicating with otherusers. In this digital world, a user's personal/banking information may need to be shared with other internet users via the social applications. This information, if not secured, can be intercepted by malicious users vulnerable to illegal use. Also, the security of the secret information in defense and other applications is of major concern. Therefore to protect information from an unauthorized access, we need robust security mechanisms. Two of the most widely used techniques for secure communication include: steganography[8] and cryptography[6]. "Steganography" is a Greek word which means "hiding writing". The word, Steganography is the combination of two parts: Steganowhich means "secret" and Graphic which means "writing". Steganography is a security mechanism of hiding sensitive information among the bits of a cover file such as an image, text, an audio file and video file in such a way that only sender and receiver know about the hidden message inside the cover file. Cryptography comes from a Greek word meaning hidden or secret writing for secure communication in the presence of an unauthorized person. Cryptography is the art of protecting sensitive information by encrypting it into an unreadable format called cipher text. The message is converted into encrypted form with the help of encryption key which is known to sender and receiver only. The receiver can decrypt this message with the help of key. However, the transmission of encrypted message is not safe because the encrypted message may easily arouse attacker's suspicion and may be intercepted or attacked easily. Dual steganography[3] is the security mechanism in which steganography and cryptography are used together. In dual steganography a secret message to be transmitted is first encrypted using encryption algorithm. Then the encrypted message (cipher text) is hidden into a cover file using steganographic technique. The cover file is then sent to the receiver. Even if a hacker suspects the presence of data into the cover file and recovers the cipher text he will still need decryption algorithm to understand the message. So using the dual steganography is much a more secure mechanism than using cryptography or steganography alone.

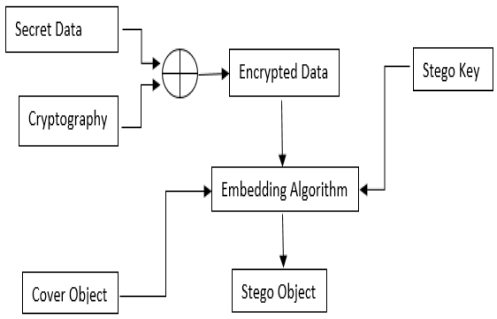

Figure 1: Dual steganography model

The Dual steganography model (Figure 1) consists of Carrier, Secret Data, StegoKey[4].

1. Carrier is the cover object in which the message is embedded.
2. Secret data can be any type of confidential data that can be plain text, other another image.
3. The secret data is encrypted into cipher data.
4. StegoKey is mainly used to ensure that only recipient having the decoding key will be able to extract the message from a cover-object.

5. By using the embedding algorithm, the secret data is embedded into the cover object in such a manner that a human perceives it as an original object.
6. Finally, the stego object which is the output of the process is the cover-object with the secretly embedded data.

Singh et al. [4] implement dual steganography as a dual layer security of data using LSB Image Steganography Method and AES Encryption Algorithm[4]. It combines both the steganography and cryptography (Encryption/ Decryption) together to achieve data security. For image steganography LSB technique is used while for encryption AES Algorithm is used.

In another work of dual steganography, Makwana et al.[5] use image steganography within video steganography. This hiding technique is specially designed for securing digital communication..

A new version of dual steganography[1]uses steganography within steganography. In this, secret data is embedded in a cover image using the status Least Significant Bit (LSB) embedding algorithm to generate a stego-image. Then stego-image is considered as secret data and it is again embedded in other cover image using the 2-D Haar-Discrete Wavelet Transform (DWT) embedding algorithm which creates a final stego–image.
A hybrid approach[2] for embedding both text and image in cover image which combines LSB and Link List method has also been developed. Encoding is performed in two ways: sequential encoding and random encoding
Govada et al.[7] implement a TextSteganography thatis more reliable and secure when compared tothe existing steganographic algorithms. It is a combination of Word shifting, TextSteganography and Synonym TextSteganography.Hence it is called as “ThreePhase Shielding Text Steganography”Dual Steganography is a state –of –art and researchers are working in this field to provide more secure communication.
We have proposed a novel algorithm of dual steganography that provides an extra level of security. The proposed algorithm combines cryptography with steganography within steganography.

II. PROPOSED WORK

In this paper, we have proposed a novel technique of dual steganography that provides a high level security to the message. In the proposed scheme, the secret message is hidden in three phases (Figure 3):-
Phase 1: A secret message is taken as an input and is encrypted using vigenere cipher technique[6].

Phase 2: The encrypted text from phase 1 and a cover text are taken as inputs and white space text steganography technique is used to hide the encrypted text in the whitespaces present in cover text.

Phase 3: The final step takes encrypted cover text from phase 2 and a cover image as input and uses LSB image steganography technique to hide the encrypted cover text in the image by embedding the bits of encrypted cover text in the RGBBGRRG order into the cover image.
The proposed data hiding algorithm works as follows(Figure 2):-

1. Encode the secret message using vigenere cipher.
2. Get the encoded text and cover text as input.
3. Convert the encoded text into binary form in block of 8 bits and get the indexes of all the whitespaces present in the cover text.
4. Now embedding the encoded text into cover text is as follows:-
    a. One whitespace for each ‘0’ bit value of encoded text.
    b. Two whitespaces for each ‘1’ bit value of encoded text.
5. Get the cover text embedded with encoded text and cover image as input.
6. Get the encryption key.
7. Add header to the beginning and normalize the encoded cover text by padding zeroes to build the 8-bits blocks in order to embed in cover image.
8. Again encrypt the encoded cover text by XORing with encryption key.
9. Hide the encrypted encoded cover text message by taking blocks of 8-bits and embedding it in red, blue and green space of image in RGBBGRRG order.
10. Prepare the final cover image as output

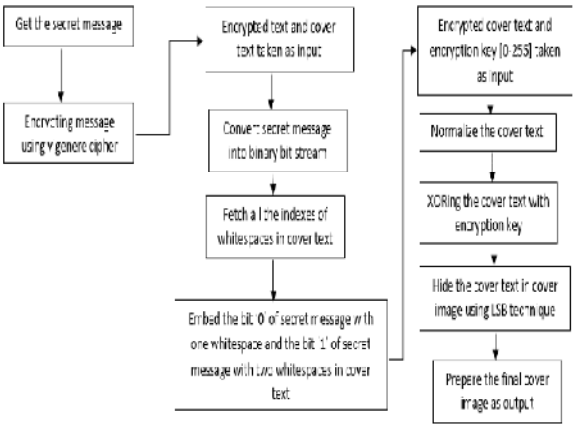

Figure 2: Flow chart showing data hiding process

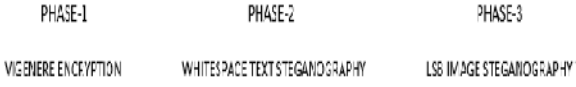

Figure 3: Three phases of data hiding

The proposed data extraction algorithm works as follows(Figure 4):-

1) Recover the encoded message from the cover image in reverse cycle of RGBBGRRG order using modulo function.
2) Recover message by using the same key used while encryption to decrypt the message set.
3) Recovered message is converted to binary form.
4) Get the index of whitespaces in recovered message bit stream.
    a. If there is a space in the message, it means bit'0' is hidden which is then stored in the resultant set.
    b. If there is consecutive space in the message, it means bit'1' is hidden which is then stored in the resultant set.
5) Secret message is recovered from cover text.
6) Decode the secret message using vigenere cipher.
7) Output the final message.

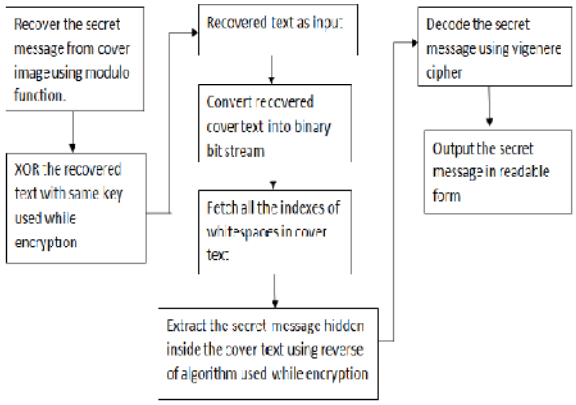

Figure 4: Flow chart showing data extraction process

III. IMPLEMENTATION AND RESULTS

The proposed algorithms are implemented in MATLAB R2009a software, version (7.8.0.347). MATLAB is a high-performance language for technical computing. The test conditions used in the implementation are as follows:-

- Capacity of cover text for hiding secret message is 41 letter maximum due to limited number of spaces present in cover text.
- Encryption key used for encrypting cover text in cover imageis integer 23.
    - Key remains constant for all the different sizes of secret messages.
    - Key remains constant for all the different sizes of cover images.

Two types of tests are performed and results (MSE and PSNR values) are shown in tables(Table 1 and Table 2):-

A. Table 1 lists the results of same cover image with different lengths of secret messages:-

- Details of cover image used, size=71.5kb, dim=600x400, format= JPEG

B. Table 2 shows the results of different cover images with same secret message:-

- Secret Message used, "Attack Korea" (12<41 Letters)

Table 1 : Showing MSE and PSNR value of different secret messages with same cover image

Secret Message	Message Length	MSE	PSNR
Attack	6<41(Letters)	0.0015	97.2540
Attack korea	12<41 (Letters)	0.0015	97.1758
Attack korea and Syria	22<41(Letters)	0.0016	97.1106
Attack korea and syria war begins	33<41(Letters)	0.0016	96.9920
Attack korea and syria beginning of ww3	39<41(Letters)	0.0016	97.0299

Table 2 : Showing MSE and PSNR value of different images with same secret message

Image	Size	Dimension	Format	MSE	PSNR
Image 1	19.6kb	199x260	JPEG	0.0068	90.7134
Image 2	60.7kb	400x600	JPEG	0.0014	97.5816
Image 3	71.5kb	600x400	JPEG	0.0015	97.1758
Image 4	91.3kb	600x474	JPEG	0.0013	98.0436
Image 5	110.0kb	600x600	JPEG	9.8333 e-004	99.0986

Figure 5 shows the original cover image used to hide the cover text embedded with secret message.

Figure 6 shows the image with hidden cover text embedded with secret message "Attack Korea".

Figure 5: Cover image before hiding secret message

Figure 6: Cover image after hiding secret message

CONCLUSIONS

Due to the exponential growth of internet users, unauthorized access of information has become one of the most significant problems. There is always a constant fear of hackers and other unwanted users for they might attack and gain access to important data, passwords or any other covert information.Therefore, to provide more security to the information at the time of communication over unsecured channel, dual steganography, an advance technique for data security is needed. In this paper, we propose a highly secure dual steganography technique which takes the secret message and hides it in three phases. First it encrypts the secret message using vigenere cipher then it applies whitespace text steganography technique and lastly it hides the cover text in cover image using LSB image steganography technique. The Final Stego-image is looking perfectly intact and has high PSNR value and low MSE value. Hence, an unintended observer will not be aware of existence of the secret message inside the cover image.

REFERENCES

[1] Manisha, DeepkiranMunjal, “Dual Steganography Technique Using Status LSB and DWT Algorithms” in proceedings of International Journal of Innovative Research in Computer and Communication Engineering, Vol.4, Issue 6, June 2016

[2] Ashwini B. Akkawar, Prof, Komal B. Bijwe, “Hybrid Approach for Embedding Text or Image in Cover Images” in proceedings of International Journal of Innovative Research in Science, Engineering and Technology, Vol.5, Issue 5, May 2016.

[3] MsKetkiThakre, Dr.NehalChitaliya,” Highly Secured Dual Steganographic Technique: A Retrospective” , International Journal of Engineering Research & Technology (IJERT)Vol. 2 Issue 10, pp. 2849-2827, October – 2013.

[4] Satwinder Singh and Varinder Kaur Attri," Dual Layer Security of data using LSB Image Steganography Method and AES EncryptionAlgorithm”, International Journal of Signal Processing, Image Processing and Pattern Recognition) Vol. 8, No. 5 pp. 259-266, 2015.

[5] JigarMakwana and S.G Chudasama, “Dual Steganography: A New Hiding Technique for Digital Communication”, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol5, Issue 4, April 2016.

[6] SonalPawar and Dr. K. James Mathai, “A Novel Approach to Design Hybrid Vigenere Caesar Cipher Encryption with Genetic Algorithm (HVCEGA) for Data Security in Cloud Computing”, International Journal of Computer Science and Network, Volume 5, Issue 4, August 2016.

[7] Sharon Rose Govada, BonuSatish Kumar , ManjulaDevarakonda and Meka James Stephen, “Text Steganography with Multi Level Shielding”, International Journal of Computer Science, Vol. 9, Issue 4, No 3, July 2012.

[8] Jasleenkour and Deepankarverma, “Steganography Techniques – a review paper”, International Journal of Emerging Research in Management & Technology, Vol. 3, Issue 5, may 2014.

★★★