Volume 4, Issue 5, May-2017, pp. 171-175 ISSN (O): 2349-7084

International Journal of Computer Engineering In Research Trends

Available online at: www.ijcert.org

Secret Data Transmission Using Combination of Cryptography &Steganography

Ajin P Thomas[1], Sruthi P.S[2], Jerry Rachel Jacob[3], Vandana V Nair[4], Reeba R [5]

[1,2,3,4,5]Sreebuddha College Of Engineering, Alappuzha , India

ajinpthomas@gmail.com,sruthips395@gmail.com,jerryjacobsbce@gmail.com,

Vandananair1295@gmail.com , Reeba,amjith @gmail.com.

Abstract :- Secure communication is when two entities are communicating and do not want a third party to listen in. For that, they need to communicate in a way not susceptible to eavesdropping or interception. Two varieties of security mechanism, cryptography and steganography are being applied. At the preceding stage, encryption is being provided to secret plain text using Vernam cipher (One-Time Pad) transposition technique. At the later stage, it transforms ciphertext into bytes and divides each byte into pairs of bits and assigns the decimal values to each pair, which is known as a master variable. Master variable value range will vary between 0 to 3. Depending upon the master patchy value, add that cipher text in the career image at Least Significant Bit (LSB) 6 th and 7 th bit location or 7 th and 8 th bit location or 7 th and 6 th or 8 th and 7 th bit location. Vernam cipher show good performance metrics regarding less CPU running time, fIle size same after Encryption and strong avalanche effect compare with all transposition cipher. After completion of embedding and sending the stego image to the receiver side, retrieving process of the cipher text from the said locations will be done. Moreover, then decryption process to get the secret plain text back will be performed using the Vernam cipher transposition algorithms.

1. Introduction

Security of information has become a tremendous term for information and communication technology nowadays. A variety of security metrics with better performance is required for the upcoming era of the internet world and big data. Secure communication includes means by which people can share information with varying degrees of certainty that third parties cannot intercept what was said. Other than spoken face-to-face communication with no possible eavesdropper, it is probably safe to say that no communication is guaranteed secure in this sense, although practical obstacles such as legislation, resources, technical issues (interception and encryption), and the sheer volume of communication serve to limit surveillance.

To accomplish security phenomenon, two techniques are used for the betterment of information secrecy, steganography over

© 2017, IJCERT All Rights Reserved

cryptography. Cryptography or cryptology is the practice and study of techniques for secure communication in the presence of third parties called adversaries. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages. Various aspects of information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include military communications, electronic commerce, ATM cards, and computer passwords.

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. The word steganography combines the Greek words steganos, meaning "covered, concealed, or protected," and graphene meaning "writing." Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter of the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

2. Literature Review

2.1 Visual cryptography and watermarking scheme

One of the new techniques in data security methods is visual cryptography allow us to share secrets between some trusted parties effectively. As with many cryptographic schemes, trust is the most difficult part. Visual cryptography provides a very powerful technique by which one secret can be distributed into two or more shares. When the shares are superimposed exactly together, the original secret can be discovered. A secret is something which is kept from the knowledge of any but the initiated or privileged. Secret sharing is a method by which a secret can be distributed among a group of the participant is allocated a piece of a secret. This piece of the secret is known as a share. The secret can be reconstructed when a sufficient number of shares are combined. While these shares are separate, no information about the secret can be accessed. That is shares are completely useless while they are separated. Pixel expansion and low contrast of the recovered image is the most important drawback in visual cryptography. Pixel expansion and low contrast level is the most important drawback in visual cryptography.

Watermarking is the technique of embedding the secret image into a cover image without affecting its perceptual quality so some process can reveal that secret image. One significant advantage of watermarking is the inseparability of the watermark (secret image) from the cover image. Some of the vital characteristics of the watermark are hard to perceive, resists ordinary distortions, endures malevolent attacks, carries numerous bits of information, capable of coexisting with other watermarks, and demands little computation to insert and extract Watermarks. Robust watermarking is used to resist un-malicious or malicious attacks like scaling, cropping, lossy compression, and so forth. Watermarking techniques can be categorized into different types based on some ways. Watermarking can be divided into Non-blind, Semi-Blind and Blind schemes based on the requirements for watermark extraction or detection. Non-blind watermarking schemes necessitate the original image and secret keys for watermark detection. The Semi-Blind schemes require the secret key) and the watermark bit sequence for extraction, whereas, the Blind schemes need only the secret keys) for extraction. Another categorization of watermarks based on the embedded data (watermark) is: visible and invisible. With visible watermarking of images, a secondary image (the watermark) is embedded in a primary image in such that it is perceptible to a human observer, whereas the embedded data is not detectable in case of invisible watermarking; nevertheless, it can be extracted by a computer program.

2.2 Data hiding using LSB method

Mangesh Kulkarni, Prasad Jagtap, Ketan Kulkarni proposed a system In which, A Least Significant Bit (called LSB) method is used for hiding the information. The 8th bit of carrier files every byte is substituted by 1 bit of secret information. The Proposed system provides a high level of security by the dual ciphering method. In this system, we are substituting the original message

© 2017, IJCERT All Rights Reserved

by using fourteen square substitution algorithms, and after that we are applying the RSA encryption algorithm on substituted text, and that encrypted cipher text is embedded in image. Hence the message is dual enciphered thus taking the security measures of information to the next level. It provides three level securities one at substitution level, second at cryptography level and third at Steganography level. If at all the intruder suspects data it is very difficult for him to steal data. The degradation in image is not noticeable. The size of the image is not increased after embedding process.

Our proposed approach can be understood by referring the following sections. In section-3 the working of Vernam cipher (One -Time Pad) transposition technique is discussed, in section-4 the embedding process, in section-5 the proposed algorithm, in section 6-conclusion.

3. Vernam Cipher

A dynamic collection of non-reoccurring characters as the input Cipher text are used in Vernam cipher algorithm. If an input cipher text for transposition is used once, will never use again for any other secret data (so the name is one-time pad). In cryptography, the one-time pad (OTP) is an encryption technique that cannot be cracked, but requires the use of a one-time pre-shared key the same size, or longer, as the message being sent. In this technique, a plaintext is paired with a random secret key (also referred to as a one-time pad). Then, each bit or character of the plaintext is encrypted by combining it with the corresponding bit or character from the pad using modular addition. If the key is truly random, is at least as long as the plaintext, is never reused in whole or in part, and is kept completely secret, then the resulting ciphertext will be impossible to decrypt or break. It has also been proven that any cipher with the perfect secrecy property must use keys with effectively the same requirements as OTP keys. Here Vernam cipher shows good performance metrics regarding less CPU running time, the length of the cipher text equals the length of the original plain text, and strong avalanche effect compares with all transposition ciphers. The steps of the algorithm have been described here.

3.1 Algorithm

- Treat each and every plain-text alphabet and symbols as a number in a rising sequence, i.e. A=O, B=1.. .. Z=25,!=27,@=28………..,;=41.
- Do the same for each character of the input cipher text also.
- Add each number which corresponds to the plain- text alphabet to the corresponding input one -time pad alphabet number.
- If the sum thus produced is bigger than 41 then perform modulus 42 to it.
- Translate each number of the sum back to the corresponding alphabet or symbol. It will give the output cipher text.

4. Embedding Process

First of all, convert the carrier image into some bytes for embedding. After that, conversion of the confidential cipher information into binary values will be done. The embedding of secret cipher data is to be done in each and every byte using logical AND and OR operation. At the receiver side, the stage image is converted into a byte array, and cipher data is extracted. Finally, the ciphertext is decrypted back to source information. First of all, convert the carrier image into some bytes for embedding. After that, conversion of the cipher information into binary values will be done. The embedding of secret cipher data is to be done in each and every byte. However, the position selection, where we have to embed the data in each byte, will be performed based on some predefined bit pattern criteria. In each bytes either the 6 & 7 or 7 & 8 or 7t & 6 or 8t & 7 bit position are used for embedding. Here we are explaining an example for better understand the procedure.

5. Proposed Algorithm

Steps 1 - Convert the carrier media file into some bytes.

Step2- Apply Vernam Cipher transposition technique on secret data to get the ciphertext.

Step3-Convert cipher text into binary values.

Step4-Check that length of carrier image is large enough to obscure the cipher text.

Step5- Embedding will be performed with the discussed embedding process.

Step6-Transmits the output stego image to the network for the recipient.

Step7- Receiver gets the hidden information by applying reverse process as sender performs on secret data.

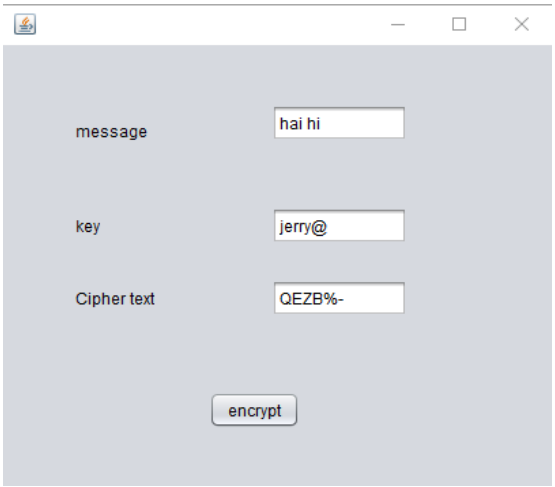
Any good steganography approach must have the following characteristics:

(i) able to obscure a sufficient amount of payload,

(ii) able to survive with search attacks,

(iii) the quality reduction of the stego image should not be noticeable and at last

(iv) able to provide at least two variety of security.

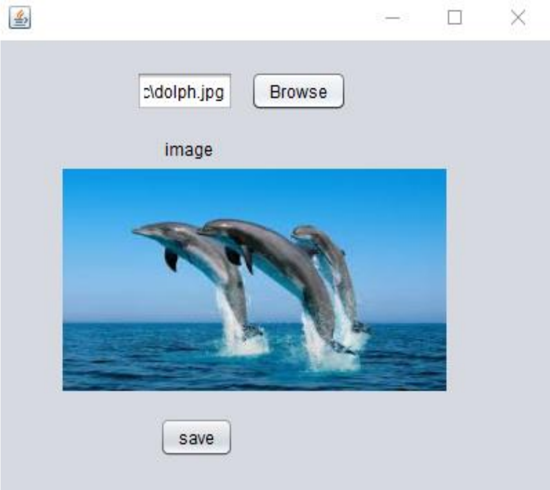


message: hai hi

key: jerry@

Cipher text: QEZB%-

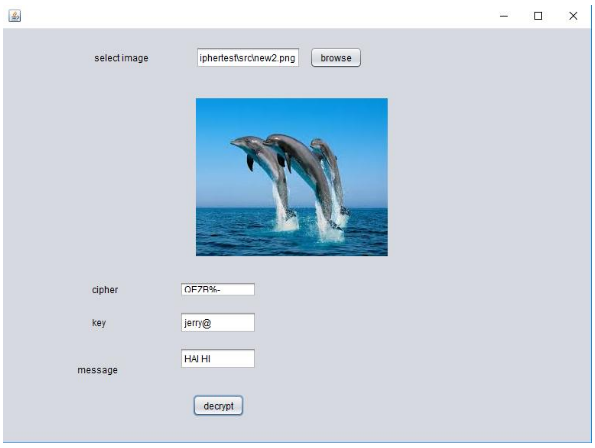
Fig 1(a): Screenshots of the screen at sender after ciphering (Vernam cipher)



:\dolph.jpg

image

Fig 1(b): Screenshots of the screen at sender after embedding.



select image: iphertest\src\new2.png

cipher: QEZB%-

key: jerry@

message: HAI HI

Fig 2: Screenshots of the screen at receiver after retrieving secret data

6. Conclusion

The proposed algorithm shows multi-transpose ability, so it is less susceptible to frequency analysis and known plaintext attacks. If this algorithm is compared to LSB and injection methods, it is better regarding intrusion prevention. In this new method, the embedding locations dynamicity is proposed, which shows a robust mechanism for variable bit positions depending on the secret message. The technique of encryption shows good performance metrics regarding less CPU running time, file size same after encryption and strong avalanche effect compare with all transposition cipher, therefore, is more suitable for short secret messages communication. It can be applicable for keeping password secure in the online banking system. This article shows bi-level security regarding steganography over cryptography. It provides better imperceptibility/quality. This algorithm is also a stronger and robust as well as secures one compared to other algorithms. No visual defects can be observed from the corresponding stego images.

References

[I] R. J. Anderson and F. A.P. Petitcolas, "On The Limits of Steganography", IEEE Journal of selected Areas in communication, 16(4), pp. 474-481,Special Issue on Copyright & Privacy protection. ISSN 0733-8716, May 1998.

[2] M. A. B. Younes and A. Jantan, "A New Steganography Approach for Image Encryption Exchange by using the LSB insertion", IJCSNS

© 2017, IJCERT All Rights Reserved

International Journal of Computer Science & Network Security, Vol 8, No 6 , pp. 247-254, June 2008.

[3] G. Swain and S .. K .. Lenka, "Steganography-Using a Double Substitution Cipher", International Journal of Wireless Communications and Networking, Volume 2, Number I, pp.35-39. ISSN: 0975-7163, June 2010.

[4] G. Swain and S. K. Lenka, " A Technique for Secure Communication using Message Dependent Steganography",Special issue of IJCCT, Vol. 2,No. 12,2010.

[5] G. Swain and S. K. Lenka, "Steganography using the Twelve Square Substitution Cipher and Index Variable" ,IEEE transactions on Image Processing, pp. 84-88, 2011.

[6] A. Nag, J. P. Singh, S. Khan and S. Ghosh," A Weighted Location Based LSB Image Steganography Technique", Springer ACC 2011, Part II, CCIS 191, pp. 620-627, 20 II.

[7] C. Maiti, D. Baksi, I. Zamider, P. Gorai and D. R. Kisku," Data Hiding in Images Using Some Efficient Steganography Techniques",Springer SIP 2011, CCIS 260, pp. 195-203, 20 II.

[8] B. Li,.,et al. "A survey on image steganography and steganalysis", Journal of Information Hiding and Multimedia Signal Processing, Vol. 2, No. 2, pp. 142172, 2011.

[9]G. Swain and S . .K .. Lenka, "A Dynamic Approach to Image Steganography Using the Three Least Significant Bits and Extended Hill Cipher" Advanced Materials Research, voI.403-408, pp.842-849,2012.

[10] S. Padmapriya, S. Saravanapriya and D. Jayachitra," Performance Analysis of Various Encryption Algorithms for Data Communication", International Journal of Computer