Volume 5, Issue 9, September 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Novel Two New Approaches for Secured Image Steganogrphy Using RGB Color Images and Cryptographic S-Des Techniques over the Internet

[1]S. Naga Mallik Raj, [2]S. Neeraja, [3]K. Sravanti
[1]Asst.Prof, Dept of CSE, Vignan's Institute of Information Technology, Duvvada, Visakhapatnam, A.P., India
[2, 3] Asst.Prof, Dept of CSE, Pydah College of Engg and Technology, Gambheeram, Vizag, A.P., India

Abstract— The growth of high-speed computer networks and that of the Internet, in particular, has increased the ease of Information Communication. Ironically, the cause for the development is also of the apprehension use of digital formatted data. In comparison with Analog media, Digital media offers several distinct advantages but this type advancement in the field of data communication in other sense has hiked the fear of getting the data intercepted at the time of sending it from the sender to the receiver, The science of securing a data by encryption is Cryptography whereas the method of hiding secret messages in other messages is Steganography, so that the secret's very existence is concealed This paper introduces two new methods where in cryptography and steganography are combined to encrypt the data as well as to hide the encrypted data in another medium so the fact that a message being sent is concealed. One method is a new way of hiding an image in another image by encrypting the image directly by S-DES algorithm using a key image and the data obtained is concealed in another image.Another method is improved LSB(least Significant bit) based Steganography technique for images imparting better information security .It presents an embedding algorithm for hiding encrypted messages in nonadjacent and random pixel locations in edges and smooth areas of images. It first encrypts the secret message, and then, embedded in the least significant byte of red, green, blue components respectively across randomly selected pixels across smooth area of image. It ensures that the eavesdroppers will not have any suspicion that message bits are hidden in the image. So by applying these two techniques we are forming two stego images. Even if Intruders hacked final stego image they will get the first stego Image. So he doesn't know where the actually information will hidden.

Keyword: Stego image, RGB Matrix, SDES,Cryptography,Steganography.

I. INTRODUCTION

In the current trends, the technologies have been advanced. Most of the individuals prefer using the internet as the primary medium to transfer data from one end to another across the internet. There are many possible ways to transmit data using the internet like: via e-mails, sending text and images, etc. In the present communication world, images are widely in use. However, one of the main problems with sending data over the Internet is the 'security' and authenticity. Data security basically means protection of data from unauthorized users or attackers. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. Encryption is one of the techniques for the information security. Image encryption is a technique that convert original image to another form that is difficult to understand. No one can access the content without knowing a decryption key. Image encryption has applications in corporate world, health care, military operations, and multimedia systems. Encryption is the process of encoding plain text message into cipher text message whereas reverse process of transforming cipher text to plain text is called as decryption. Cryptography consists of encryption and decryption techniques. In this paper we are implementing both Cryptography and Steganography.

Cryptography and steganography are cousins in the spy craft family: the former scrambles a message so it cannot be understood, the latter hides the message so it cannot be seen. A cipher message, for instance, might arouse suspicion on the part of the recipient while an invisible message created with steganographic methods will not. In. However, steganography and cryptography differ in the way they are evaluated: steganography fails when the "enemy" is able to access the content of the cipher message, while cryptography fails when the "enemy" detects that there is a secret message present in the steganographic medium. The disciplines that study techniques for deciphering cipher messages and detecting hide messages are called cryptanalysis and steganalysis. cryptography at the same time using images as cover objects for steganography and as keys for cryptography

II. PURPOSE OF CRYPTOGRAPHY

Cryptography provides a number of security goals to ensure the privacy of data, non alteration of data and so on. Due to the great security advantages of cryptography it is widely used today. Following are the various goals of cryptography.

2.1 ***Confidentiality****:* Information in computer is transmitted and has to be accessed only by the authorized party and not by anyone else.

2.2 ***Authentication****:* The information received by any system has to check the identity of the sender that whether the information is arriving from a authorized person or a false identity.

2.3 ***Integrity****:* Only the authorized party is allowed to modify the transmitted information. No one in between the sender and receiver are allowed to alter the given message.

2.4 ***Non Repudiation****:* Ensures that neither the sender, nor the receiver of message should be able to deny the Transmission.

2.5 ***Access Control****:* Only the authorized parties are able to access the given information.

III. EXISTING SYSTEM

In Existing system several methods are there to hide the information in the image to obtain stego image. And they send stego image directly into medium. Someone they encrypt the stego image and they send encrypted stego image into medium. So they are chances to the intruders to get back the hidden information.

IV. PROPOSED SYSTEM:

In proposed system we are hiding the information into a image to form a stego image. (**cover image + secret key + hidden information = stego image).** For this we are proposing improved LSB(least Significant bit) based Steganography technique for images imparting better information security .It presents an embedding algorithm for hiding encrypted messages in nonadjacent and random pixel locations in edges and smooth areas of images. It first encrypts the secret message, and then, embedded in the least significant byte of red, green, blue components respectively across randomly selected pixels across smooth area of image. It ensures that the eavesdroppers will not have any suspicion that message bits are hidden in the image .After that cryptography will fallows, for that we using SDES to encrypt the stego image. We obtain Encrypted stego image. Instead of sending Encrypted stego image directly, again we proposing to hide this Encrypted stego image into another cover image. Finally we sending Stego image2 (which contains hidden information i.e Encrypted stego image). So if Intruders attacks on our stego image2 they will get encrypted stego image. Even though if they decrypt the Encrypted stego image, they will get stego image1. So it is very difficult to the intruders to see the original hidden information and which image it was hidden. Let us discuss the process step by step.

V. AT SENDER SIDE

FIRST STEP:

It is a new approach to substitute LSB of RGB true color image. The new security conception hides secret information within the LSB of image where a secret key encrypts the hidden information to protect it from unauthorized users. In general, in LSB methods, hidden information is stored into a specific position of LSB of image, To hide hidden information we have to take a cover image. This cover image is divided into three matrices (Red, Green and Blue) as shown in Fig.1 The secret key and Hidden Information is converted into 1D array of bit stream. For the first three Pixels of Cover Matrix following procedure is applies: Secret key and Red matrix are used for decision making to replace hidden information into either Green matrix or Blue matrix. Each bit of secret key is XOR with each LSB of Red matrix. The resulting XOR value decides that the First bit of hidden information will be placed with either LSB of Green matrix or Blue matrix. Next 2nd bit of secret key and LSB of second pixel of Green matrix are XORed such that decision will makes to hide the second bit of hidden information into blue matrix or Red Matrix.

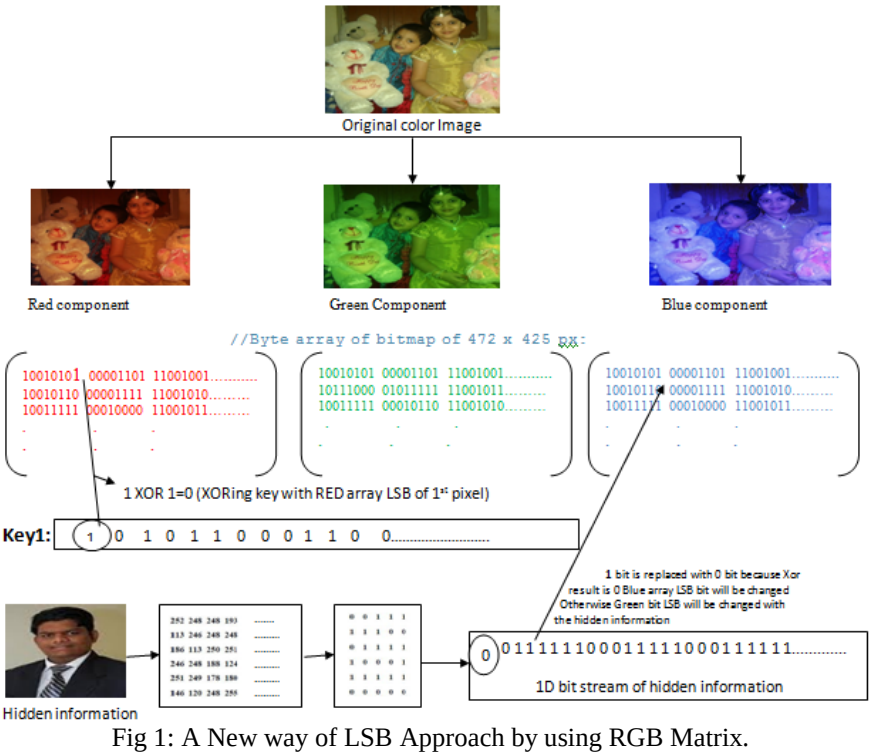

Fig 1: A New way of LSB Approach by using RGB Matrix.

Like that cycle will repeats until all bits of hidden information will be hidden into the Three RGB Matrixes. In the below Fig 1, Three Matrixes of RGB components will taken from the original image. And Secret key and hidden information was converted into 1D matrix. First bit of Key is 1 and it is XORed with LSB of first pixel of Red Matrix. Result is 0. So we have to hide the 1st bit of hidden information is 0 and it is replaced with the LSB of First pixel of Blue Matrix i.e 1. So 1 is replaced with 0. If result is 1, then we have to replace LSB of First pixel of Green Matrix. Like that cycle will repeat to until all bits of hidden information will hide**.**

At last this end of this process after combining of RGB images first stego image will be formed. Which is similar to the original image. With the human eye we cannot differentiate the original image and stego image. Which was shown in fig 2.

Fig 2: After Combining of RGB images which contains hidden information then we obtain Stego Image

SECOND STEP CRYPTOGRAPHY:

After a new way of LSB approach completes encryptions will fallows. i.e we encrypt the stego image with the key by using the SDES method. We obtain encrypted stego image as shown in below figure 3.

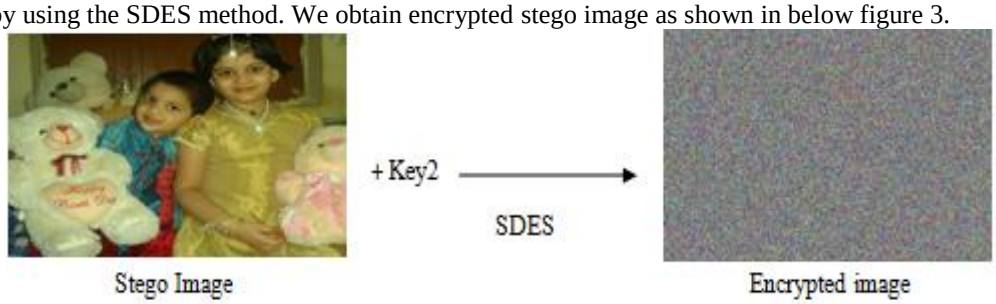

Fig 3: Result of SDES encryption.

THIRD STEP: NORMAL LSB APPROACH:

Instead of transmitting encrypted image directly into Medium. We have to hide this into the another image, so second stego image will be formed. Which is more secure, that intruders never guess where the original information in these images. In this step we are following normal LSB approach. i.e the bits of encrypted image will be hide into the LSB bit of image which was shown in below figure 4.

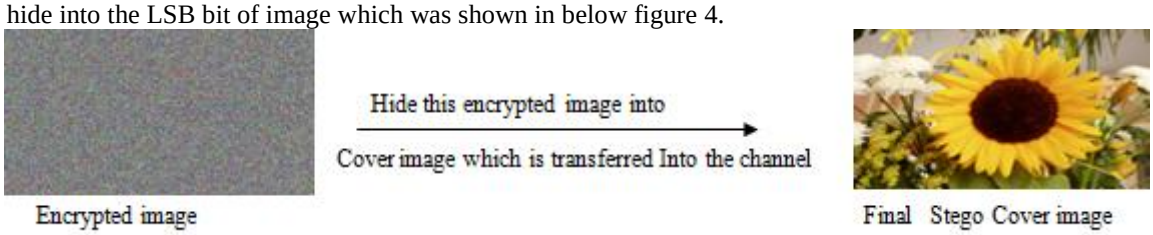

Fig 4: Formation of Final stego image with normal LSB approach.

FORTH STEP:

The final stego image will be transmitted into the medium.

VI. AT RECEIVER SIDE(STEP BY STEP PROCESS)

1)At receiver side receiver receives the final stego image

2)Receiver extracts the bits of LSB from the stego cover image , by that receiver extracts encrypted image from the stego image

3)Then receiver applies SDES method with the same key(A Key which was used in encryption) on Encrypted image we obtain First stego image.

4)We applied our proposed LSB approach on stego image with the key. Then we obtain actually hidden information.Let us discuss step by step

i)First bit of key is Xored with LSB bit of first pixel of RED Matrix.

ii)If result is 1 then we extract the LSB bit of first pixel of Green matrix. Otherwise we extract from the Blue matrix.

iii)Like that cycle will repeats until all the bits are extracted from the RGB matrix.

5) let us see the entire process at receiver side with results in the below figure 5.

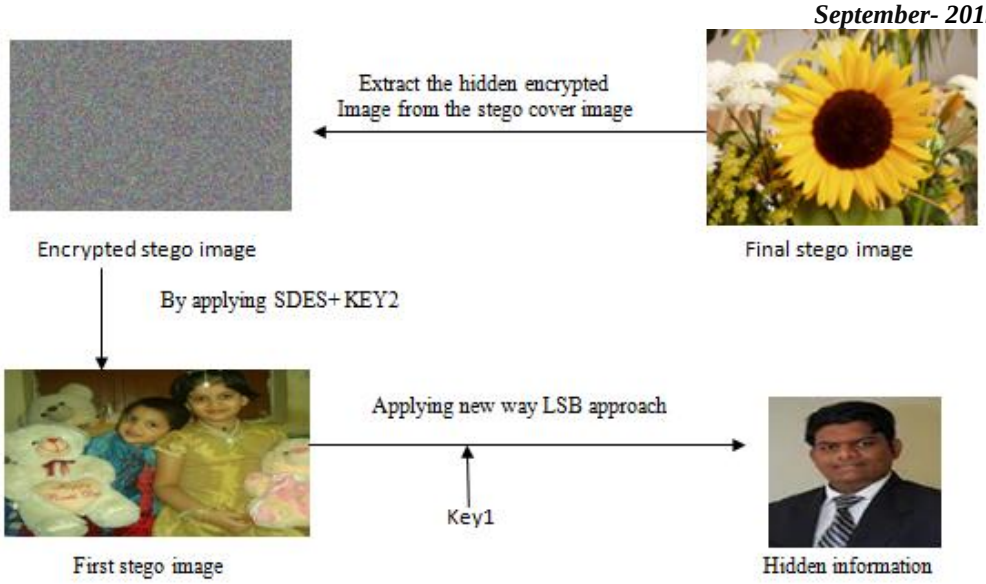

Fig 5: The entire process from receiver side

VII. CONCLUSION

In this paper we have presented a novel method for integrating in an uniform model cryptography and steganography. We have proven that the presented LSB in a new way method is an effective steganographic method as well as a theoretically unbreakable cryptographic one. Strength of our system resides in the new concept of key image. Involving two images (the cover and the key) in place of only one (the cover) we are able to change the cover coefficients randomly.. The proposed approach has many applications in hiding and coding messages within standard medias, such as images or videos.. So by applying these two techniques we are forming two stego images. Even if Intruders hacked final stego image they will get the first stego Image. So he doesn't know where they actually information will hidden.

REFERENCES

[1] Digital Image Processing. [Courtesy of http://en.wikipedia.org/wiki/ Digital_image_processing]

[2] Suresha D, Sathisha M S, Alok Ranjan, Prasanna Kumara, "Implementation of Protected Routing to Defend Byzantine Attacks for MANET's ",2012 International Journal of Advanced Research in Computer Science, Volume 3, No. 4, July- August2012, ISSN No. 0976-5697.

[3] Andreas Tønnesen, "Mobile Ad-Hoc Networks", 802.11 illustrations by LarsStran. [Courtesy of http://www.olsr.org/docs/wos3-olsr.pdf] [6] Dipesh Patel, Dr. Rakesh Nagi, "Ad hoc Wireless Networks", A Presentation October 17, 2001. [Courtesy of http://www.acsu.buffalo.edu/~nagi/courses/ 684/adhoc.pdf]

[4] F. Hartung and M. Kutte "Information hiding-a survey," Proceedings of the IEEE: Special Issue on Identification and Protection of Multimedia Content, Volume: 87 Issue:7, pp. I062- I078, July. 1999.

[5] M. Hossain, S.A. Haque, F. Sharmin, "Variable Rate Steganography in Gray Scale Digital Images Using Neighborhood Pixel Information", Proceedings of 2009 12th International Conference on Computer and Information Technology (ICCIT 2009) 21-23 December 2009, Dhaka, Bangladesh.

[6] Namita Tiwari and Madhu Shandilya, "Secure RGB Image Steganography from Pixel Indicator to Triple Algorithm-An Incremental Growth", International Journal of Security and Its Applications, Vol. 4, No. 4, pp. 53-62, 2010.

[7] Koyi Lakshmi Prasad and T. Ch. Malleswara Rao, "A Novel Secured RGB LSB Steganography with Enhanced Stego-Image Quality", International Journal of Engineering Research and Applications, Vol. 3, No. 6, pp. 1299-1303, 2013.

[8] Mamta Juneja and Parvinder S. Sandhu, "An Improved LSB based Steganography Technique for RGB Color Images", 2nd International Conference on Latest Computational Technologies, pp. 10-14, 2013.

[9] Mohammad Tanvir Parvez and Adnan Abdul-Aziz Gutub, "RGB Intensity Based Variable-Bits Image Steganography", IEEE Asia-Pacific Services Computing Conference, pp. 1322-1327, 2008.

