IJRRECS/November 2015/Volume-3/Issue-11/4945-4949 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

AN AUTHENTICATION SCHEME FOR AUTHENTICATING RELIABILITY OF SECRET MESSAGE

S V L Raga Divya[1], S.Hemanth Chowdary[2], T.Shesagiri[3]

[1]M.Tech, Dept of CSE, Joginpally BR Engineering College, Hyderabad, T.S, India

[2]Associate Professor, Dept of CSE, Joginpally BR Engineering College, Hyderabad, T.S, India

[3]Associate Professor, Dept of CSE, Joginpally BR Engineering College, Hyderabad, T.S, India

ABSTRACT:

The increased possibilities regarding modem communications require particular means of security especially on computer network. Steganography is a technique of embedding information within cover image devoid of causing important variations towards cover image. The most important objective of Steganography is to communicate in totally unnoticeable way and to keep away from drawing of suspicion to transmit hidden data. In our work we introduce an effective method that conceals secret message or else information into spatial domain of cover image. We suggest an image Steganography that authenticate data reliability that is being conveyed to receiver and the system will validate whether attacker has attempted to change, erase or forge secret data in stego-image. The proposed method will embed concealed information within spatial domain of cover image and make use of two special coefficients of Discrete Wavelet Transform domain to confirm reliability of secret information from stegoimage. Our method can authenticate integrity of secret message that is concealed in the carrier by means of Discrete Wavelet Transform.

Keywords: Steganography, Discrete Wavelet Transform domain, Hidden data, Stego-image, Spatial domain, Computer network, Secret message.

1. INTRODUCTION:

Steganography is a Greek word and Steganos means covered and graphy denotes writing. Steganography indicates actually covered writing. With traditional methods of communication, Steganography is used to perform hidden messages and communicates in unnoticeable way and to keep away from drawing of suspicion to transmit hidden data. When the method of Steganography causes to imagine that there is a secret data in carrier medium, then method turn into ineffective. We include image steganalysis which is a process to detect potentially concealed information from specified image and hence discovers useless to covert messages, thus breaking Steganography [1]. Steganalysis is classified as passive as well as active forms. Steganalysis scheme attempts to prevail over Steganography by means of detection of concealed information as well as extracting. Passive method identifies presence or else absence of secret message in observed image or recognizes embedding algorithm type. The active method will estimate several message properties of embedding algorithm. To attain information security as well as privacy, secret data that gets fixed in a carrier all the way through random permutation by means of verification code. In our work we suggest an image Steganography that authenticate data reliability that is being conveyed to receiver [2][3]. The proposed technique will validate whether attacker has attempted to change, erase or forge secret data in stego-image. The proposed technique will embed concealed information within spatial domain of cover image and make use of two special coefficients of Discrete Wavelet Transform domain to confirm reliability of secret information from stego-image.

2. METHODOLOGY:

In the recent times, Steganography as well as Steganalysis are significant areas of study that involve several applications. The former will communicate in unnoticeable way and to keep away from drawing of suspicion to transmit hidden data. Image steganalysis is a process to detect potentially concealed information from specified image. Steganalysis method attempts to overcome the approach of Steganography by means of detection of concealed information as well as extracting. When the method of Steganography causes to imagine that there is a secret data in carrier medium, then method turn into ineffective. In our work we present Steganography method that conceals

secret message or else information into spatial domain of cover image. Steganography will offer high level of confidentiality along with security by means of combining by means of cryptography. Our technique can authenticate integrity of secret message that is concealed in the carrier by means of Discrete Wavelet Transform. The proposed technique will validate whether attacker has attempted to change, erase or forge secret data in stego-image. It will embed concealed information within spatial domain of cover image and make use of two special coefficients of Discrete Wavelet Transform domain to confirm reliability of secret information from stegoimage. For unbeaten recovery of concealed information communication channel have to be perfect but for actual communication channel, there is error while recovering of concealed information and is measured by means of Bit Error Rate. Until recent times, methods of information hiding techniques have received extremely less attention from research community than cryptography. Cryptography as well as steganography are extensively used in data hiding and have gained important concentration from industry as well as academia in recent times [4]. Former will conceal actual data but latter will conceal extremely fact that data is concealed. Steganography will provide high level of confidentiality along with security by means of combining by means of cryptography.

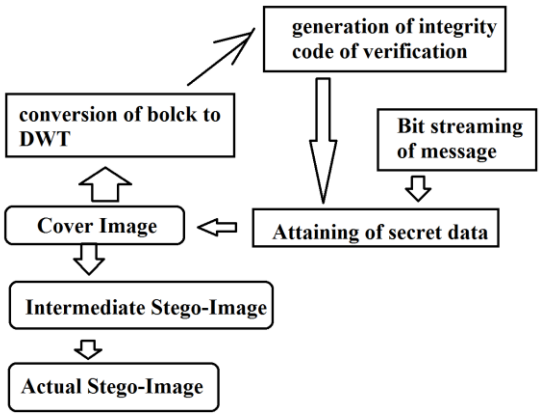

Fig1: an overview of embedding process.

3. AN OVERIVEW OF PROPOSED SYSTEM:

The network security has turned out to be more significant since number of data that is being exchanged on Internet increases hence privacy as well as data integrity are necessary to defend against illegal access. It has resulted in unstable expansion of information hiding area, that include applications for instance copyright security for digital media, fingerprinting. These applications regarding information hiding are relatively diverse. Steganography communicates in unnoticeable way and to keep away from drawing of suspicion to transmit hidden data. Steganalysis is

classified as passive as well as active and the passive method identifies presence or else absence of secret message in observed image or recognizes embedding algorithm type. The active method will estimate several message properties of embedding algorithm. Steganography was used to in secret communicate information amongst people and the technique will hide secret message within host data set as well as its presence is unnoticeable and is consistently communicated towards a receiver. In our work we present Steganography method that conceals secret message or else information into spatial domain of cover image. Our technique can authenticate integrity of secret message that is concealed in the carrier by means of Discrete Wavelet Transform. The proposed means confirm reliability of secret message from stego image. We produce a Verification code by means of using two alternate coefficients of Discrete Wavelet Transform domain to confirm reliability of secret information that are diagonally positioned [5]. The proposed technique will validate whether attacker has attempted to change, erase or forge secret data in stego-image. The proposed technique will embed concealed information within spatial domain of cover image and make use of two special coefficients of Discrete Wavelet Transform domain to confirm reliability of secret information from stegoimage. The proposed means confirm reliability of secret message from stego image. We produce a Verification code by means of using two alternate coefficients of Discrete Wavelet Transform domain to confirm reliability of secret information that are diagonally positioned [6]. This Verification code is permuted by means of secret message and is afterwards fixed in spatial domain of cover image. In the process of embedding process, after changing present row in cover image to block form, Discrete Wavelet Transform is functional to blocks. In this block two special coefficients that are diagonal are selected to produce Verification code and the obtained Verification code is subsequently permuted all the way through secret message that is to be fixed within cover image. The permutation is managed by means of secret key to attained secret information. The secret key will make a decision of the method to permute verification code by means of secret message to produce secret information. Consequently attained secret data is grouping of secret message as well as Verification code. The embedded image is at

the present middle stego image. The same procedure of making of verification code is followed in support of intermediary stego-image. Code is fixed towards intermediate stego-image to outline real image that is to be transmitted to receiver.

4. CONCLUSION:

Steganography as well as Steganalysis are the two areas of research that are important when consistent and safe information exchange is necessary. In our work we provide steganography method that conceals secret message or else information into spatial domain of cover image. The projected method will validate whether attacker has attempted to change, erase or forge secret data in stego-image. The technique will embed concealed information within spatial domain of cover image and make use of two special coefficients of Discrete Wavelet Transform domain to confirm reliability of secret information from stegoimage. It can validate integrity of secret message that is concealed in the carrier by means of Discrete Wavelet Transform. The proposed means confirm reliability of secret message from stego image. We construct a Verification code by means of using two alternate coefficients of Discrete Wavelet Transform domain to confirm reliability of secret information that are diagonally positioned.

REFERENCES

[1] R. D. Jiri Fridrich and M. Long, "Steganalysis of LSB encoding in Color Images," in International Conference on signal Processing, pp. 1279– 1282, Jan 2000.

[2] C. T. R. Lisa M. Marvel and C. G. Boncelet, "Hiding Information in Images," in International Conference on Image Processing, pp. 396–398, Mar 1998.

[3] N. F. Johnson and S. Jajodia, "Steganalaysis: The investigaton of Hidden information," in International Conference on Information Technology, pp. 113–116, Jun 1998.

[4] H. Y. Shaohui Liu and W. Gao, "Steganalysis of Data Hiding Techniques in Wavelet Domain," in International Confernce on Information Technology, pp. 119–121, August 2004.

[5] V. M. potdar and E. Chang, "Gray Level Modification Steganography for Secret Communication," in International Conference on image Processing, pp. 223–228, April 2004.

[6] A. H. S. Gopalkrishna Reddy Tadiparthi and S. Mukkamala, "Defeating the Current Steganalysis Techniques," in International Conference on Information Technology, pp. 224–228, April 2004.