International Journal For Technological Research In Engineering
Volume 3, Issue 10, June-2016 *ISSN (Online): 2347 - 4718*

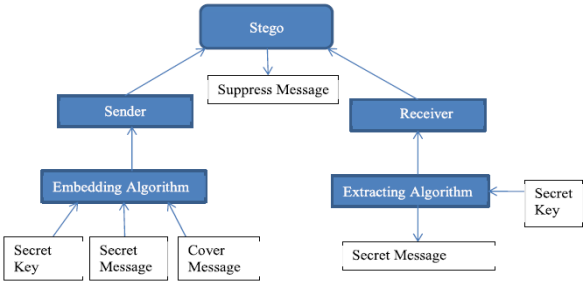
NIESA SCHEME FOR ENCRYPTED TEXT STEGNOGRAPHY

Geeta Grewal[1], Pallavi Sharma[2]
[1]Electronics and Communication Department, ITS, Bhiwani, Haryana, India
[2]Computer Science Department, T.I.T&S Bhiwani, Haryana, India

Abstract: ***The work used here mainly focuses on implementing stegnography for images for promoting Security and quality of an image .This is improved using the difference between two pixels of an stego-pixel. The data over the network need to transfer securely. An LSB is implemented here for pixel hiding. In this technique stego least significant bits of cover image is selecting by current pixel of stego image. RGB image based pixels have 24 bits in which 8 bits represent red color, 8 bit to show green color and last 8 bits are for blue color. The proposed approach enhances the robustness of data. In this technique encrypt a text file into an image file using algorithm (NIESA) that do process of encryption.***
KEYWORDS: ***NIESA Technique, Encryption, Stegnography, Image.***

I. INTRODUCTION

Steganography is the art and science of writing hidden messages in such a way that no-one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. The medium where the secret data is hidden is called as cover medium, this can be image, video or an audio file. Any stego algorithm removes the redundant bits in the cover media and inserts the secret data into the space. Higher the quality of video or sound more redundant bits are available for hiding.Generally, messages will appear to be something else: images, articles, shopping lists, or some other cover text and, classically, the hidden message may be in invisible ink between the visible lines of a private letter. In terms of computer security, steganography is really nothing new, as it has been around since the times of ancient Rome. For example, in ancient Rome and Greece, text was traditionally written on wax that was poured on top of stone tablets. If the sender of the information wanted to obscure the message - for purposes of military intelligence, for instance - they would use steganography: the wax would be scraped off and the message would be inscribed or written directly on the tablet, wax would then be poured on top of the message, thereby obscuring not just its meaning but its very existence.



It is an effective means of hiding data, thereby protecting the data from unauthorized or unwanted viewing. But stego is simply one of many ways to protect the confidentiality of data. It is probably best used in conjunction with another data-hiding method. When used in combination, these methods can all be a part of a layered security approach. Some good complementary methods include:

- Encryption - Encryption is the process of passing data or plaintext through a series of mathematical operations that generate an alternate form of the original data known as ciphertext. The encrypted data can only be read by parties who have been given the necessary key to decrypt the ciphertext back into its original plaintext form. Encryption doesn't hide data, but it does make it hard to read!
- Hidden directories (Windows) - Windows offers this feature, which allows users to hide files. Using this feature is as easy as changing the properties of a directory to "hidden", and hoping that no one displays all types of files in their explorer.
- Hiding directories (Unix) - in existing directories that have a lot of files, such as in the /dev directory on a Unix implementation, or making a directory that starts with three dots (...) versus the normal single or double dot.
- Covert channels - Some tools can be used to transmit valuable data in seemingly normal network traffic. One such tool is Loki. Loki is a tool that hides data in ICMP traffic (like ping).

Types of Steganography –

1. Text Steganography: It consists of hiding information inside the text files. In this method, the secret data is hidden behind every nth letter of every words of text message. Numbers of methods are available for hiding data in text file. These methods are i) Format Based Method; ii) Random and Statistical Method; iii) Linguistics Method.

2. Image Steganography: Hiding the data by taking the cover object as image is referred as image steganography. In image steganography pixel intensities are used to hide the data. In digital steganography, images are widely used cover source because there are number of bits presents in digital representation of an image.

3. Audio Steganography: It involves hiding data in audio files. This method hides the data in WAV, AU and MP3 sound files. There are different methods of audio steganography. These methods are i) Low Bit Encoding ii) Phase Coding iii) Spread Spectrum.

4. Video Steganography: It is a technique of hiding any kind of files or data into digital video format. In this case video

(combination of pictures) is used as carrier for hiding the data. Generally discrete cosine transform (DCT) alter the values (e.g., 8.667 to 9) which is used to hide the data in each of the images in the video, which is unnoticeable by the human eye. H.264, Mp4, MPEG, AVI are the formats used by video steganography.

II. LITERATURE REVIEW

Steganographic methods have been proposed in literature and most of which are performed in pixel domain. However major contribution is in the domain of Image Steganography. The existing methods are mainly based on LSB where LSBs of the cover file are directly changed with message bits.

In [7] Fillatre. L, Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption, IEEE Transactions on Signal Processing, Volume 60a is a robust image steganography technique based on LSB insertion and RSA encryption technique has been used.

Masud K. S.M. Rahman, Hossain, M.L., A new approach for LSB based image steganography using secret key, in Proceedings of 14th International Conference on Computer and Information Technology (ICCIT-2011) [8] has proposed a LSB technique for RGB true color image by enhancing the existing LSB substitution techniques to improve the security level of hidden information.

Other Examples of LSB schemes can be found in [9] Hema Ajetrao, Dr. P.J.Kulkarni and Navanath Gaikwad, A Novel Scheme of Data Hiding in Binary Images,and [10] Sachdeva S. and Kumar A, Colour Image Steganography Based on Modified Quantization Table.

Whereas EzStego developed by achado [11] embed information into an image in the GIF format. It sorts the palette to ensure the difference between two adjacent colors is visually indistinguishable

. Tseng and Pan [12] presented a data hiding scheme in 2-color images, it embeds the information in any bit where at least one of the adjacent bits is the same as the original unchanged bit. Kawaguchi et. al.

E. Kawaguchi and R. O. Eason, Principle and applications of BPCS-Steganography, in Proceedings of SPIE Int'l Symp. on Voice, Video, and Data Communications,[13] proposes bit plane complexity segmentation(BPCS) method to embed information into the noisy areas of the image. These techniques are not limited to the LSB.

III. PROPOSED METHODOLOGY

In NIESA technique two types of approaches are used to promote security in data.

- Encryption
- Steganography

In first approach, encryption is done by converting the text file and image into binary code. In second approach, Steganography is applied by a new technique which is called "NIESA".

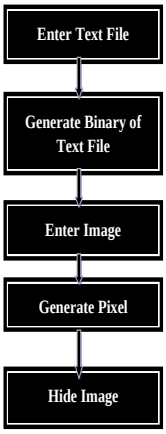
Following steps are implemented for the NIESA insertion -

- Read the container file and the text byte to byte.
- Convert both the files into bits.
- Replace the least significant bit of 11th byte of the image file with the first text bit.
- Continue this process till the end of text file.
- Store the resultant byte in the steganographed file.
- Then Save the stego image for use.

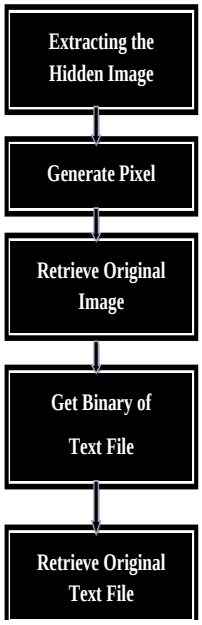
Following steps are implemented for the retrieval of data from a file

- Read the new stego image file byte to byte.
- Collect the LSB of every byte.
- Extract the LSBs into a new byte array and convert that byte array into a new text file
- This text file is the original text.

The process of embedding is shown below –



The process of extracting is shown below -

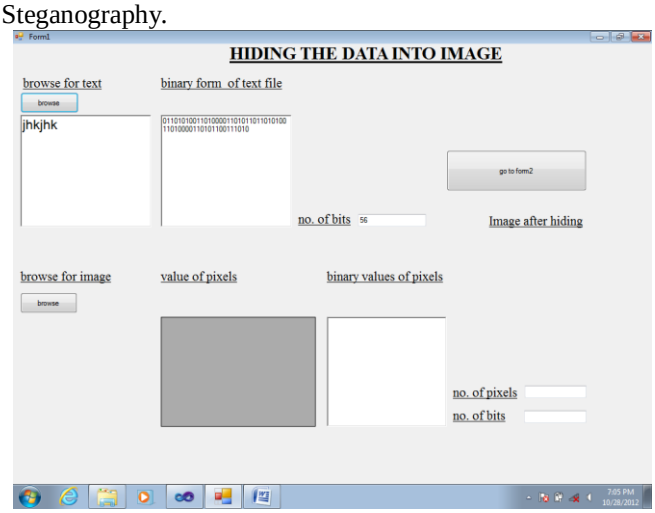


IV. RESULT

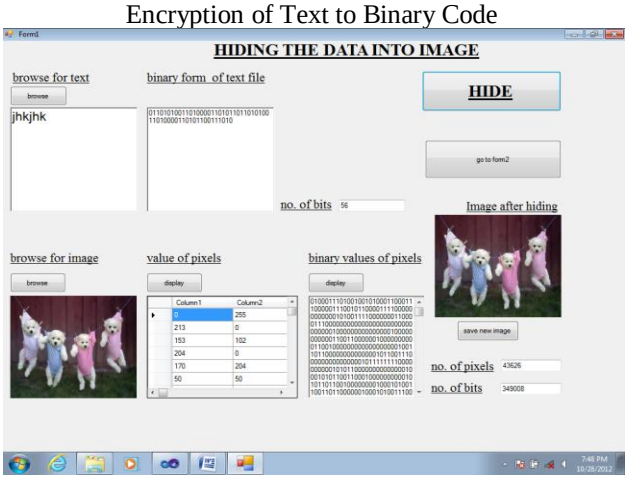
In the proposed system, NIESA Scheme is employed for enhancing security.

The following figures shows the operations:
(a) Encryption of Text to Binary code.

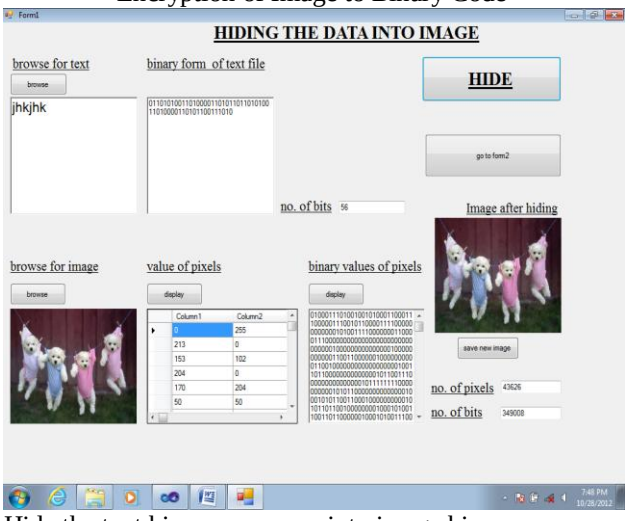
(b) Encryption of image to binary code.
(c) Hide the text binary sequence into image binary sequence using NIESA technique.
(d) Extracting the text in binary format from the image using NIESA technique.
The Research is carried on text as well as on image with purposed algorithm which includes Encryption and Steganography.



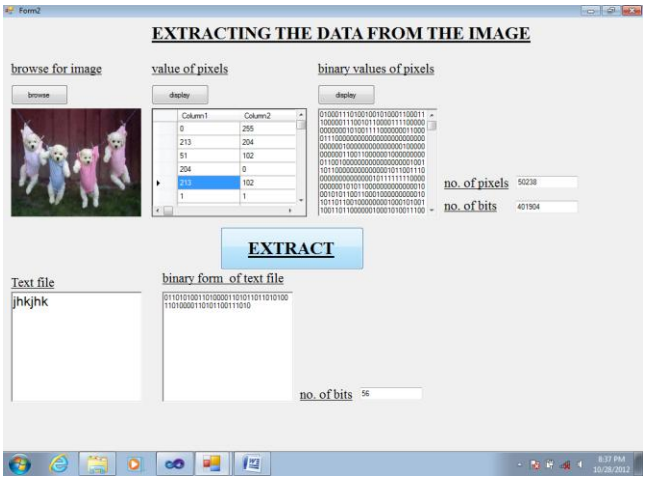
Encryption of Text to Binary Code



Encryption of Image to Binary Code



Hide the text binary sequence into image binary sequence using NIESA technique.



Extract the text in binary format from the image using NIESA.

V. CONCLUSION

Steganography is a powerful and effective method of hiding data that has been used throughout history. To uncover different devices tactics this method is used, but the first step are awareness that such methods even exist. There are many good reasons as well to use this type of data hiding that include methods like watermarking or a more secure central storage method for such things as passwords, or key processes. The technology used here is easy to use and difficult to detect. The more that you know about its features and functionality, the more ahead you will be in the game. Used tool is compatible with different formats like .bmp and .gif of images. The quality of the comparison cover image does not degrade with data hidden in it as long as the ratio of the size of comparison the data and the size of the cover image are about 1:11.

ACKNOWLEDGMENT

The author is thankful to Sunil Kumar, Professor of Electronics & Communication Engineering Department of Institute of Technology & Sciences, Bhiwani (Haryana), India for giving suggestions during work that enabled us to present this work.

REFERENCES

[1] E. Cole and R.D. Krutz, Hiding in Plain Sight: Steganography and the Art of Covert Communication, Wiley Publishing, Inc., ISBN 0-471-44449-9, 2003.
[2] Stefan Katzenbeisser and Fabien A. P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House Books, ISBN 1-58053-035-4, 1999.
[3] D. Stanescu, M. Stratulat, B. Ciubotaru, D Chiciudean, R. Cioarga and M. Micea, Embedding Data in Video Stream using Steganography, in 4th International Symposium on Applied Computational Intelligence and Informatics, SACI-2001, pp. 241-244, IEEE, 2007.
[4] Feng Pan, Li Xiang, Xiao-Yuan Yang and Yao

Guo, Video Steganography using Motion Vector and Linear Block Codes, in IEEE 978-1-4244-6055-7/10/, pp. 592-595,2010.

[5] A. Westfield, and A. Pfitzmann, Attacks on Steganographic Systems, in Proceedings of 3rd Info. Hiding Workshop, Dresden, Germany, Sept. 28−Oct. 1, pp. 61-75, 1999.

[6] J. Fridrich, R. Du, and L, Meng, Steganalysis of LSB Encoding in Color Images, in Proceedings of ICME 2000, Jul.-Aug. 2000, N.Y., USA.

[7] Fillatre. L, Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption, IEEE Transactions on Signal Processing.

[8] Masud K. S.M. Rahman, Hossain, M.L., A new approach for LSB based image steganography using secret key, in Proceedings of 14th International Conference on Computer and Information Technology (ICCIT-2011), pp.-286-291, Dec. 2011.

[9] Hema Ajetrao, Dr. P.J.Kulkarni and Navanath Gaikwad, A Novel Scheme of Data Hiding in Binary Images, in International Conference on Computational Intelligence and Multimedia Applications, Vol.4, pp. 70-77, Dec. 2007.

[10] Sachdeva S. and Kumar A, Colour Image Steganography Based on Modified Quantization Table, in Proceedings of Second International Conference on Advanced Computing & Communication Technologies (ACCT-2012), pp. 309-313, 2012.

[11] Y. C Tseng and H. K Pan, Data Hiding in 2-color Image in IEEE Transactions on computers.

[12] E. Kawaguchi and R. O. Eason, Principle and applications of BPCS-Steganography, in Proceedings of SPIE Int'l Symp. on Voice, Video, and Data Communications.

[13] Mritha Ramalingam, Stego Machine Video Steganography using Modified LSB Algorithm, in World

[14] Academy of Science, Engineering and Technology 74 2011, pp. 502-505, 2011.

[15] Juan Jose Roque and Jesus Maria Minguet, SLSB: Improving the Steganographic Algorithm LSB, in the 7th International Workshop on Security in Information Systems (WOSIS 2009.

[16] A.K. Bhaumik, M. Choi, R.J. Robles and M.O. Balitanas, Data Hiding in Video in International Journal of Database Theory and Application Vol. 2, No. 2, pp. 9-16, June 2009.

[17] J. J. Chae, B. S. Manjunath, Data Hiding in Video, Proceedings of the 6th IEEE International Conference on Image Processing, pp.311-315, 1999.

[18] Melih Pazarci, Vadi Dipcin, Data Embedding in Scrambled Digital Video, in Proceedings of the 8th IEEE International Symposium on Computers and Communication, pp. 498-503, 2003.

