ISSN 0976 – 1411

Available online at www.internationaleJournals.com

International eJournals

International eJournal of Mathematics and Engineering 227 (2013) 2216 - 2222

INTERNATIONAL eJOURNAL OF MATHEMATICS AND ENGINEERING

www.InternationaleJournals.com

EFFICIENT METHOD OF AUDIO STEGANOGRAPHY BY SYMMETRIC ENCRYPTION KEY WITH ENHANCED SECURITY

[1]Tarun Dhar Diwan, [2]Bhoopendra Dhar Diwan and [3]Aaqib Rashid

[1, 3]Department of Engineering, [2]Department of Basic Sciences
Dr. C. V. Raman University, Bilaspur (C.G), India
tarunctech@gmail.com, bddiwan@gmail.com, jahangeer.lone@gmail.com

***Abstract*—**In this paper In this paper, the proposed method hides the secret message based on searching about the identical bits between the secret messages and image pixels values. The performed computer simulation demonstrates the high efficiency of the proposed technique and the analytical comparative analysis indicates a number of advantages in comparison with the existed steganography software. For hiding secret information in images, there exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points The first to employ hidden communications techniques -with radio transmissions- were the armies, because of the strategic importance of secure communication and the need to conceal the source as much as possible. Nowadays, new constraints in using strong encryption for messages are added by international laws, so if two peers want to use it, they can resort in hiding the communication into casual looking data. This steganography application software provided for the purpose to how to use any type of image formats to hiding any type of files inside their. The master work of this application is in supporting any type of pictures without need to convert to bitmap, and lower limitation on file size to hide, because of using maximum memory space in pictures to hide the file. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet. For hiding secret information in images, there exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points the first to employ hidden communications techniques because of the strategic importance of secure communication and the need to conceal the source as much as possible. Nowadays, new constraints in using strong encryption for messages are added by international laws, so if two peers want to use it, they can resort in hiding the communication into casual looking data. This problem has become more and more important just in these days, with which around thirty of the major - with respect to technology countries in the world methods are discussed and analyzed based on the ratio between the number of the identical and the non identical bits between the pixel color values and the secret message values This property is used for proposed image encryption and for steganography to increase the security level of the encoded image and to make it less visible.

***Keywords*:** surveillance information, segmenting, Object tracking, significant percentage, auto-calibration.

1. INTRODUCTION

The goal of steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second secret message present. The only missing information for the enemy is the short easily exchangeable random number sequence, the secret key, without the secret key, secure operating system design, a term which refers to all communication paths that cannot easily be restricted by access control mechanisms. In an ideal world we would all be able to sent openly encrypted mail or files to each other with no fear of reprisals[1,2].. However there are often cases when this is possible, either because the working company does not allow encrypted email or the local government does not approve of encrypt communication (a reality in some parts of the world)[3].The effective and appropriate Steganography algorithm must be selected that able to encode the message in more secure technique. Then the sender may send the Stego file by email or chatting, or by other modern techniques. The Stego file is the carried message with the secret information[4]. After receiving the message by the receiver, he can decode it using the extracting algorithm and the same password used by the sender [5]. The Steganography system scenario is shown in the Figure 1.

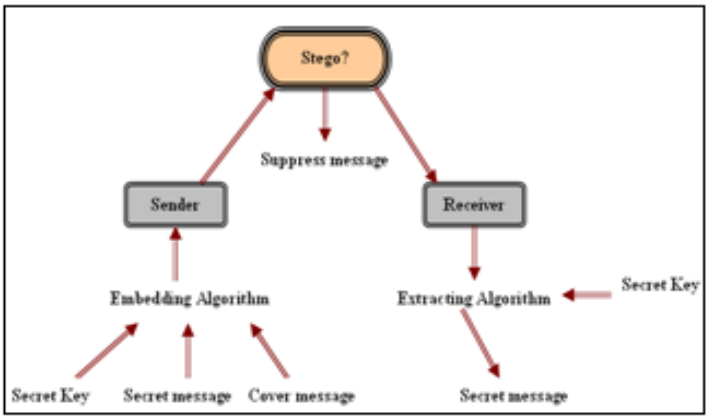


Figure 1: Steganography System Scenario

Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret [4,6].Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated [7]. The strength of steganography can thus be amplified by combining it with cryptography.

2. LITERATURE REVIEW

We Steganography is a word derived from the ancient Greek words steganos, which means covered and graphic, which in turn means writing. Steganography is an art and science of information hiding and invisible communication. It's unlike cryptography, where the goal is to secure communications from an eavesdropper by make the data not understood, steganography techniques strive to hide the very presence of the message itself from an observer so there is no knowledge of the existence of the message in the first place. In some

situations, sending encrypted information will arouse suspicion while invisible information will not do so. Both sciences can be combined to produce better protection of the information. In this case, when the steganography fails and the message can not be detected if a cryptography technique is used too. Hiding information inside audio is a popular technique nowadays [6,8].The two primary issues of concern for steganographers are robustness and transparency. Robustness means that the hidden message will actually survive long enough to be extracted by the intended recipient. If we are dealing with some kind of physical system, we need to make sure the message will be physically unharmed by the steganographic embedding process, and by whatever process will deliver the message to the recipient. In an electronic system, robustness is related to whether or not the communication will survive the effects of common channels through which it may pass, such as the addition of noise, signal degradation, or digital compression [9].Hiding information inside audio files can be done in several different ways. Using the least-significant bit modifications will usually not create audible changes to the sounds. Another method involves taking advantage of human limitations. It is possible to encode messages using frequencies that are inaudible to the human ear. Using any frequencies above 20.000 Hz, messages can be hidden inside sound files and will not be detected by human checks. Also, a message can be encoded using musical tones with a substitution scheme. For example, a F tone will represent a 0 and a C tone represents a 1. A normal musical piece can now be composed around the secret message or an existing piece can be selected together with an encoding scheme that will represent a message [8,10].

3.OBJECTIVES

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet. For hiding secret information in images, there exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points.So we prepare this application, to make the information hiding more simple and user friendly.

4. EXPERIMENT & METHODOLOGY

The encrypt module is used to hide information into the image; no one can see that information or file. This module requires any type of image and message and gives the only one image file in destination. The decrypt module is used to get the hidden information in an image file. It take the image file as an output, and give two file at destination folder, one is the same image file and another is the message file that is hidden it that. Before encrypting file inside image we must save name and size of file in a definite place of image. We could save file name before file information in LSB layer and save file size and file name size in most right-down pixels of image [11]. Writing this information is needed to retrieve file from encrypted image in decryption state.

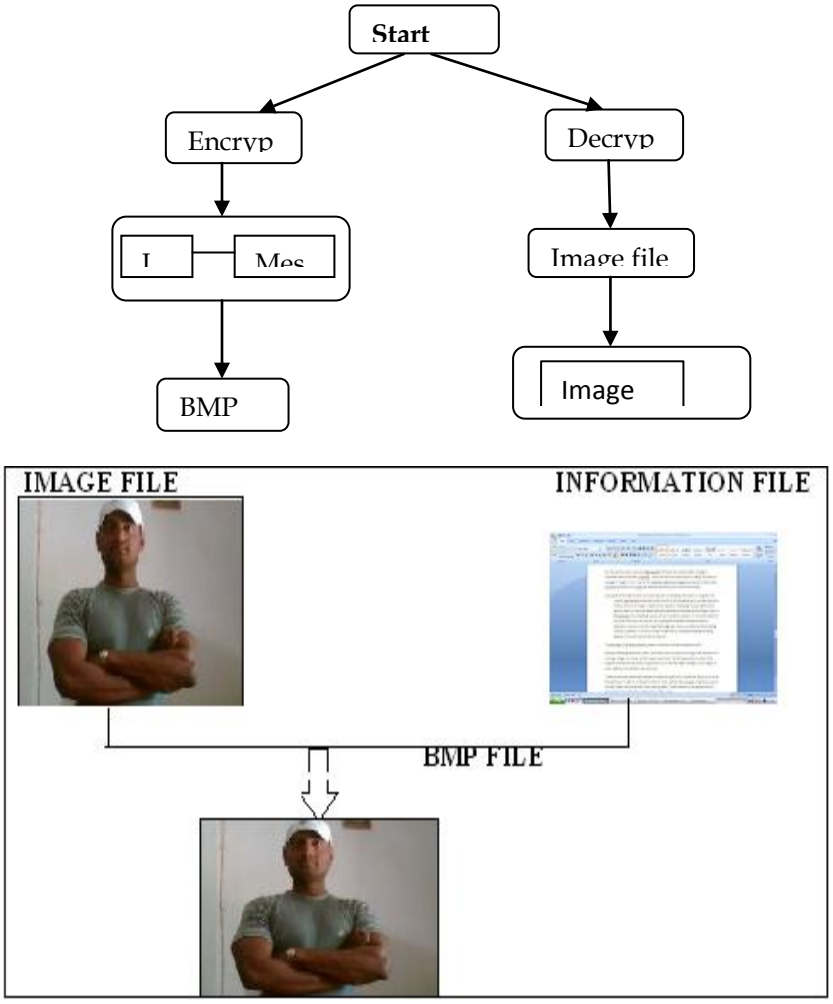


Figure2.
Encryption processes in image file, information file, bmp file Representation of the System

The performed computer experiments show that just phase information makes possible to reconstruct image uniquely. The phase of the given image in combination with the averaged amplitude spectrum obtained from the group of images gives the satisfactory results in the most practical important cases. Therefore, adding some component in the phase spectrum of the image one can essentially change the initial image structure[12]. The above phenomenon could be efficiently used for image encryption. Moreover, the localized communication noise is spread over all reconstructed image that makes it invisible opposite the above mentioned approach where localized noise conditions local noise associated with blocking effect.

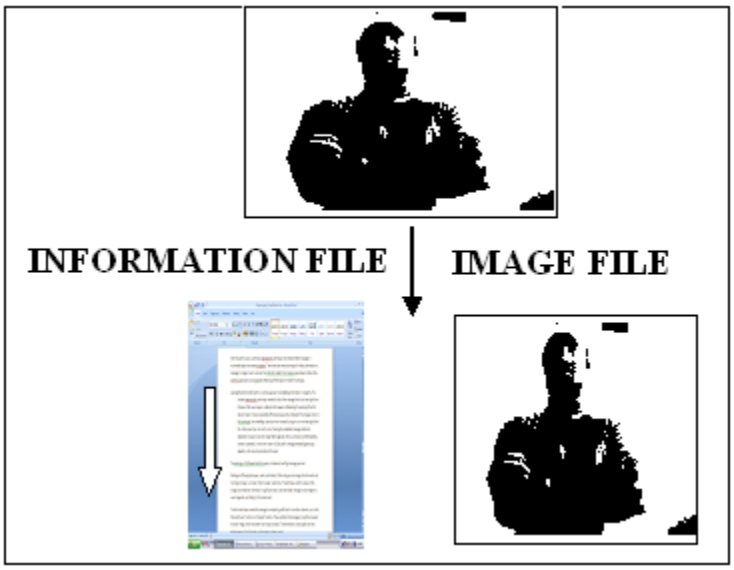


Figure3.
Decryption processes in image file, information file, bmp file Representation of the System

We describe how it is possible to combine the techniques of encryption, data hiding and steganography in image. a new problem is trying to combine in a single step, compression, encryption and data hiding[13]. So far, few solutions have been proposed to combine image encryption and compression for example. Nowadays, a new challenge consists to embed data in encrypted images. Since the entropy of encrypted image is maximal, the embedding step, considered like noise, is not possible by using standard data hiding algorithms. A new idea is to apply reversible data hiding algorithms on encrypted images by wishing to remove the embedded data before the image decryption [14]. In This method we encrypt the original image with two share mechanism then embed the encrypted image with patient information by using lsb lossless data embedding technique with data hiding key after that for more security [15].

5. RESULT

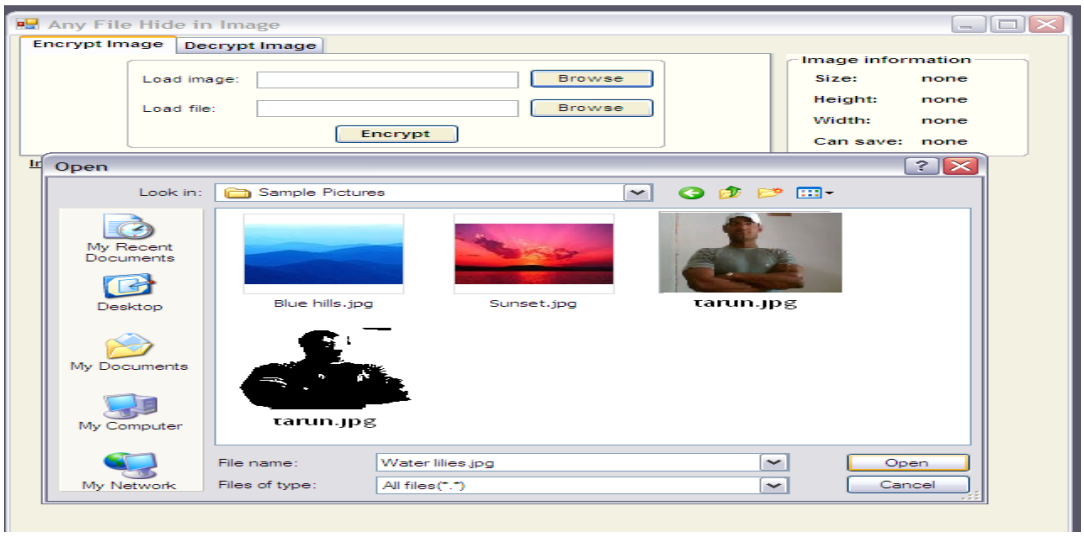
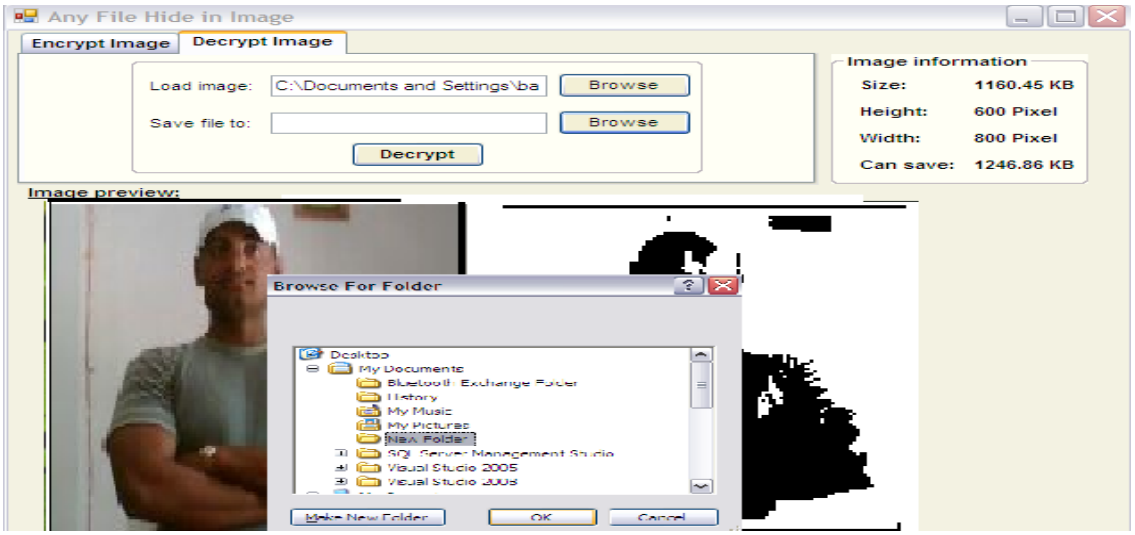


Figure 4. For load image click on button “Browse” that is next to the Load Image textbox. The file open dialog box will displays as follows, select the Image file, which you want to use hide information and click on Open button.



frameRate = get(trafficObj,'FrameRate');
implay(taggedCars,frameRate);

Figure5.

Visualize Results Get the frame rate of the original video and use it to see tagged Cars in implay

6. DISSCUTATION AND CONCLUSATION

We develop and adopt the concept of matlab programming for different object detection and compared their detection quality and time-performance. The adaptive background subtraction scheme gives the most promising results in terms of detection quality and computational complexity to be used in a real-time surveillance system with cameras. However, no object detection algorithm is perfect, higher level semantic extraction steps would be used to support object detection step to enhance its results and eliminate inaccurate segmentation. the proposed whole-body object tracking algorithm successfully tracks objects in consecutive frames. our tests in sample applications show that using nearest neighbor matching scheme gives promising results and no complicated methods are necessary for whole-body tracking of objects. also, in handling simple object occlusions, our histogram-based correspondence matching approach recognizes the identities of objects entered into an occlusion successfully after a split. however, due to the nature of the heuristic we use, our occlusion handling algorithm would fail in distinguishing occluding objects if they are of the same size and color. also, in crowded scenes handling occlusions becomes infeasible with such an approach, thus a pixel-based method, like optical flow is required to identify object segments accurately.

REFERENCES

[1] Xinpeng Zhang]ieee signal processing letters, VOL. 18, NO. 4, APRIL 2011 255 Reversible Data Hiding in Encrypted Image.
[2] M. Naor, and A. Shamir,Visual Cryptography Advances in Cryptology – Eurocrypt‘94 Proceeding, LNCS Vol. 950, Springer-Verlag,1995, pp. 1-12.
[3] Jamil, T., “Steganography: The art of hiding information is plain sight”, IEEE Potentials, 18:01, 1999

[4] Wang, H & Wang, S, “Cyber warfare: Steganography vs. Steganalysis”, Communications of the ACM,47:10, October 2004
[5] Anderson, R.J. & Petitcolas, F.A.P., “On the limits of steganography”, IEEE Journal of selected Areasin Communications, May 1998
[6] Marvel, L.M., Boncelet Jr., C.G. & Retter, C., “Spread Spectrum Steganography”, IEEE Transactions on image processing, 8:08, 1999
[7] Dunbar, B., “Steganographic techniques and their use in an Open-Systems environment”, SANSInstitute, January 2002
[8] Artz, D., “Digital Steganography: Hiding Data within Data”, IEEE Internet Computing Journal, June 2001
[9] Simmons, G., “The prisoners problem and the subliminal channel”, CRYPTO, 1983
[10] Chandramouli, R., Kharrazi, M. & Memon, N., “Image steganography and steganalysis: Concepts and Practice”, Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003
[11] M. Naor, and A. Shamir, ―Visual Cryptography, Advances in Cryptology – Eurocrypt‘94 Proceeding ,LNCS Vol. 950, Springer-Verlag, 1995, pp. 1-12.
[12] M. Naor and A. Shamir, ―Visual Cryptography II: Improving the Contrast Via the Cover Base, Cambridge Workshop on Protocols, 1996.
[13]“An Authentication Server in Java Implementation of an Encryption”, Framework Model and DES Algorithm in Java Leandro Batista de Almeida, Walter Godoy Jr., Jotio Luiz Kovaleski , 0-7803-5030-8/98/$10.00 1998 IEEE.
[14] “Efficient Method Of Audio Steganography By Modified Lsb Algorithm And Strong Encryption Key With Enhanced Security”, 1r Sridevi, 2dr. A Damodaram, 3dr. Svl.Narasimham, Journal of Theoretical and Applied Information Technology © 2005 - 2009 JATIT.
[15] “Introduction to MATLAB-7 for Engineers”, Palm, William J, Mc Graw Hill, 2005

AUTHOR BIOGRAPHIES

TARUN DHAR DIWAN RECEIVED HIS MASTER OF ENGINEERING (COMPUTER TECHNOLOGY AND APPLICATION) DEGREE FROM CHHATTISGARH SWAMI VIVEKANANDA TECHNICAL UNIVERSITY –BHILAI, INDIA, AND MASTER OF PHILOSOPHY (GOLD MEDAL LIST) FROM DR. C.V. RAMAN UNIVERSITY. HE IS CURRENTLY AN HOD & MTECH CO-ORDINATOR DEPTT. OF ENGINEERING AT THE DR.C.V.RAMAN UNIVERSITY-BILASPUR, INDIA. HIS CURRENT RESEARCH WORK ARTIFICIAL INTELLIGENT, IMAGE PROCESSING AND SOFTWARE ENGINEERING.