INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS…..

Strong Encryption Key with Enhanced Security of image Steganography by Modulus operator Method

TARUN DHAR DIWAN[1], **SOMYA YASH** [2]

[1]Dr.C.V.RAMAN UNIVERSITY, BILASPUR, INDIA
ASSISTANT PROFESSOR
DEPTT.OF ENGINEERING (CSE)
taruncsit@gmail.com

[2]Dr.C.V.Raman University, Bilaspur, India,
M.TECH SCHOLAR
soumyashwant@gmail.com

Abstract: *Steganography isa special technque implimented in images. The most popularin it is cover objects. In the domain of digital images various image file formats exist, most of them have specific applications Secret messages embedded inside digital cover media like text, images, audio, video or protocols depending upon the requirement and choice of the sender. Compared with the other types of steganography, the image steganography is most widely used. The reason behind the popularity of image steganography is the large amount of necessary information present in the images that can be easily changed to hide secret messages inside them. It can take advantage of the limited power of the human visual system. The Steganography technique is the perfect supplement for encryption that allows user to hide large amounts of information within an image. Thus, it is often used in conjunction with cryptography so that the information is completely protected; first it is encrypted and then it is hidded so that an adversary first has to find the hidden information before decryption take place The problem with cryptography is the encrypted message.It is obviously the codes, that are the secret messages found in the text file ''Message.txt'' into the JPEG image file ''Cover.jpg'' and produces the stego image ''Stego.jpg''. The idea behind this is to abuse the recognition of EOF (End of file).*

Keywords: *Steganography technique, secret information, image encryption, interfacing context, secret communication, modulus operator.*

1. INTRODUCTION

Steganography is one of many techniques that are used to hide secret information to prevent any attackers to make damage in this information or use it in illegal form. Steganography can be defined as the technique used to lay data or other secret information inside some other object commonly referred to as cover, by changing its properties. The purpose of steganography is to create a secret communication path between two parties such that any person in the middle cannot detect its existence the attacker should not gain any information about the hidden data by simply looking at cover file or segos file. Steganography is the art of hiding information in ways that prevent anyone from detecting the hidden messages. Steganography, derived from Greek, which means "covered writing."It includes a vast array of secret communications methods that Makes the message's very existence. These methods include invisible inks, microdots, character arrangement, digital signatures, covert channels, and spread spectrum [1, 2].The basic model of steganography uses a cover object (any object that can be used to hold secret information inside), the secret messages (the secret information that is to be sent to some remote place secretly), a segos key that is used to encode the secret message to make its detection difficult and a steganography technique (the procedure to hide secret message inside cover object). The outcome of the process is the segos object which is the object that has the secret message covered inside. This segos object is sent to the receiver where receiver will get the secret data out from the segos image by using decoding algorithm/technique [3].Recently, steganography is implemented by using digital media. Secret message is embedded inside digital cover media like text, images, audio, video or protocols depending upon the requirement and choice of the sender. Compared with the other types of steganography, the image steganography is most widely used [4].The reason behind the popularity of image steganography is the large amount of necessary information present in the images that can be easily altered to hide secret messages inside them, and because it can take advantage of the limited power of the human visual system (HVS). With the prolonged growth of strong graphics power in computer and the research being put into image based steganography, a good technique of image steganography aims at three aspects. First one is capacity (the maximum data that can be stored inside cover image) [5]. Second one is the imperceptibility (the visual quality of stego-image after data hiding) and the last is robustness.The main terminologies used in the steganography systems are: the cover message, secret message, and secret key and embedding algorithm [6]. The cover message is the carrier of the message such as image, video, audio, text, or some other digital media.The secret message is the information which is needed to hide in suitable digital media. The secret key is usually used to embed the message depending on the hiding algorithms. The embedding algorithm is the way or the idea that usually use to lay the secret information in the cover message. The segos file is the carried message with the secret information [7]. After receiving the message by the receiver, he can decode it using the extracting algorithm and the same password used by the sender [8]. The steganography system scenario is shown in the figure 1.

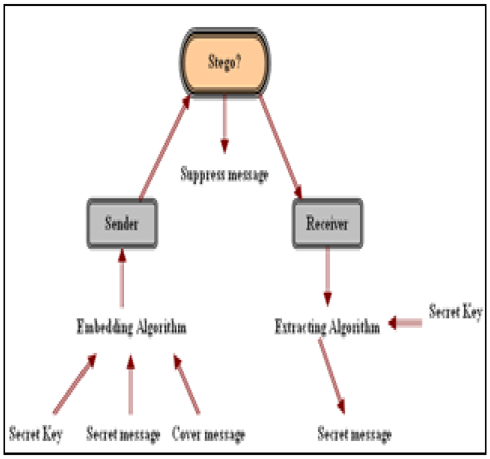


Figure 1: Steganography System Scenario

Today steganography is mostly used in computers with digital data being the carriers and networks being the high speed delivery channels. Steganography differs from cryptography in the way that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret [9,10].Steganography and cryptography are both used to protect information from unwanted parties but not a single technology is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated [11]. The strength of steganography can thus be amplified by combining it with cryptography.

2. PREVIOUS RESEARCH

A literature review of current research investigating 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 making the data ununderstoodable, 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 places, sending encrypted information will cause suspicion while invisible

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS…..

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 cannot be detected then the cryptography technique is used too. Hiding information inside audio is a popular technique nowadays [12].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 that the message will be physically unharmed by the steganographic embedding process, and it will be their responsibility to deliver the message by what ever means to the recipient. In an electronic system, robustness is related to whether the communication will survive or not to the effects of common channels through which it may pass, such as the addition of noise, signal degradation, or digital compression [13].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 substitutional scheme. For example, an 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 encoded scheme that will represent a message [14].

2.1 PURPOSE OR RESEARCH

Research and Application Challenges

The purpose of this research is to develop a Steganography which 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 complex than others, but each of them have respective strong and weak points. So we prepare this application, to make the informations hiden simpler and user friendly.

3. EXPERIMENT & METHODOLOGY

The proposed system is based on the secret messages, which are directed in the least two significant bits in the image pixels, which affect the image resolution, and reduce the image quality and make the image easy to hit.This method is already been hit and broken. Therefore a new technique that is able to make the secret message more secure and enhance the quality of the image is proposed [1,15].The proposed method hides the secret message based on searching about the identical values between the secret messages and image pixels, see the proposed method is used to hide the secret messages by using any byte is a number N from 0 to 255. This means that we can expand it in binary: ifr_1, g_1, b_1, a_1, r_2, g_2, b_2, a_2 {0, 1}, then we can write N as

$N = r_1 + g_1 2 + b_1 2^2 + a_1 2^3 + r_2 2^4 + g_2 2^5 + b_2 2^6 + a_2 2^7$

Then if (R_1,G_1,B_1,A_1) and (R_2,G_2,B_2,A_2) are two adjacent pixels in a 32 bmp image, we overwrite.

% = modulus operator

(R_1,G_1,B_1,A_1) - (R_1,G_1,B_1,A_1) % 2 + (r_1,g_1,b_1,a_1)

(R_2,G_2,B_2,A_2) - (R_2,G_2,B_2,A_2) % 2 + (r_2,g_2,b_2,a_2)

The algorithm used in our steganographic program. Suppose, for example, that two adjacent image pixels are (255,255,255,0) and (255,255,255,0), and we wish to hide the data N = 18. Then by our algorithm, Notice how little the pixels change to hide the data; to the human eye, both pixels are still white.

N =18
r1 = N % 2 = 18 % 2 = 0
T = r1 = 0
g1 = (N - T)/2 % 2 = (18 - 0)/2 % 2 = 9 % 2 = 1
T = T + 2 * g1 = 0 + 2*1 = 2
b1 = (N - T)/4 % 2 = (18 - 2)/4 % 2 = 4 % 2 = 0
T = T + 4 * b1 = 2 + 4*0 = 2
a1 = (N - T)/8 % 2 = (18 - 2)/8 % 2 = 2 % 2 = 0

T = T + 8 * a1 = 2 + 8*0 = 2
r2 = (N - T)/16 % 2 = (18 - 2)/8 % 2 = 1 % 2 = 1
T = T + 16 * r2 = 2 + 16*1 = 18
g2 = (N - T)/32 % 2 = (18 - 18)/2 % 2 = 0 % 2 = 0
T = T + 32 * g2 = 18 + 2*0 = 18
b2 = (N - T)/64 % 2 = (18 - 18)/64 % 2 = 0 % 2 = 0
T = T + 64 * b2 = 18 + 4*0 = 18
a2 = (N - T)/128 % 2 = (18-18)/128 % 2 = 0 % 2 = 0

So, the new pixels are
(255,255,255,0) - (255,255,255,0) % 2 + (0,1,0,0)
= (255,255,255,0) - (1,1,1,0) + (0,1,0,0)
= (254,255,254,0)
(255,255,255,0) - (255,255,255,0) % 2 + (1,0,0,0)
= (255,255,255,0) - (1,1,1,0) + (1,0,0,0)
= (255,254,254,0)

4. IMPLEMENTATION AND RESULT

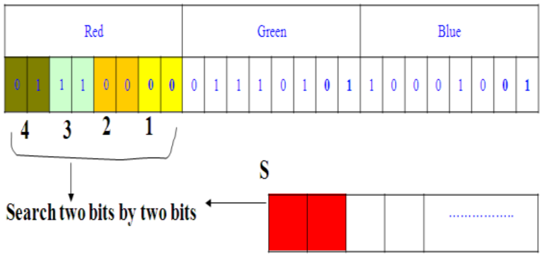
Inputs: RGB image, secret message and the password.

Output: Stego image.

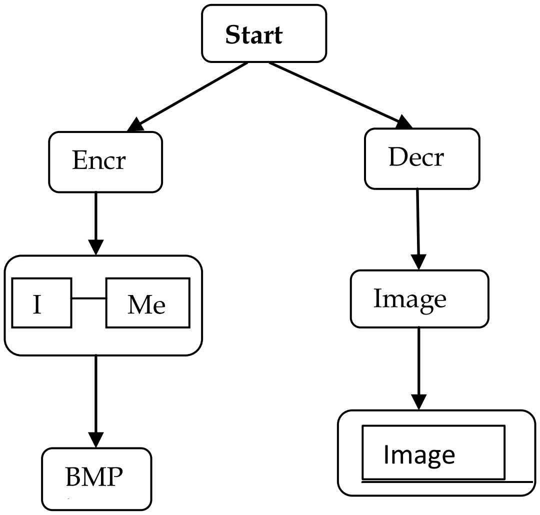
From the beginning it scans the image row by row and encodes the secret message in binary. Then it checks the size of the image and the size of the secret message.

Start sub-iteration choose one pixel of the image randomly divide the image into three parts (Red, Green and Blue parts) hide two by two bits of the secret message in each part of the pixel by searching its identical. If the identical is satisfied then set the image with the new values. Otherwise hide in the two least significant bits and set the image with the new values save the location of the hiding bits in binary table. end sub-iteration 1.set the image with the new values and save it.

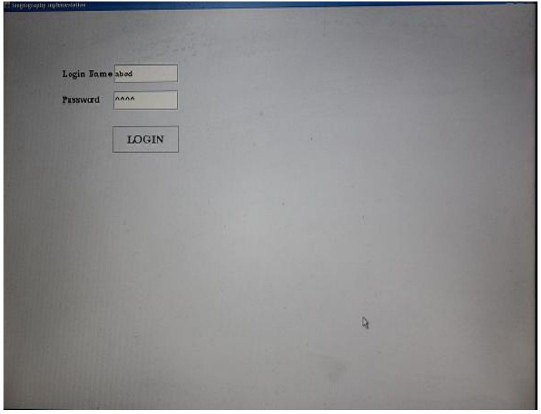
End



Red								Green								Blue							
0	1	1	1	0	0	0	0	0	1	1	1	0	1	0	1	1	0	0	0	1	0	0	1



There is demo of my project Steganography, as all of we know Steganography is hiding a message from the normal human eyes, here we are performing Steganography with the help of digital jpeg picture and encryption key applying through modulus operator. Step by step follow the process of encryption and decryption. Only Authorized person can operate this because this all protected with Login Id nd Password.

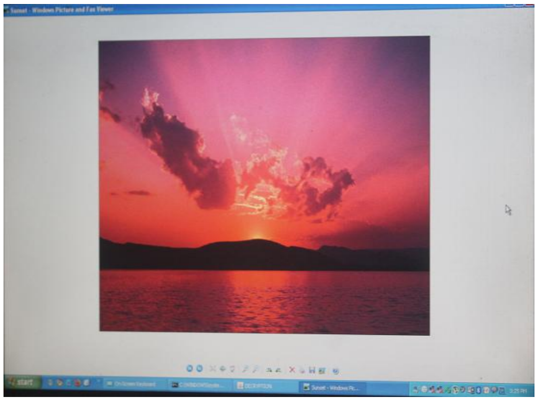


Steganography implementation

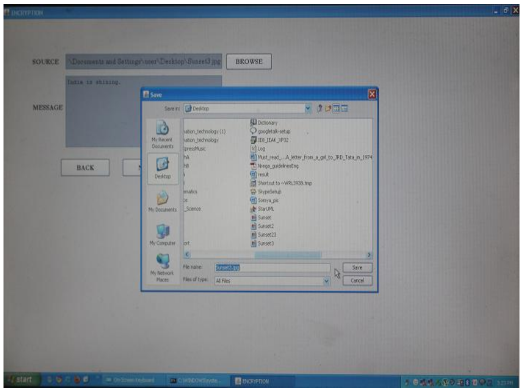
Login Name abcd

Password ^^^^

After entering password it gives u choices weather u want to perform encryption or decryption. As we can find as following pic



As in following picture we can see data encrypted by encryption key in the picture on the system and saved file can be transferd by the mail to the another authorized person.



SOURCE: \Documents and Settings\user\Desktop\Sunset3.jpg

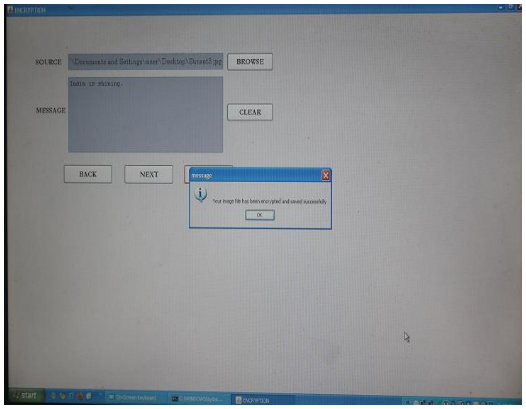
India is shining.

Save in: Desktop

File name: Sunset3.jpg

Files of type: All Files

The performed computer experiments show that just phase information makes it possible to reconstruct image uniquely. The phase of the given image in combination with the averaged amplitude spectrum obtained from the group of images giving the satisfactory results in the most practical and important cases



SOURCE: \Documents and Settings\user\Desktop\Sunset3.jpg

India is shining.

Your image file has been encrypted and saved successfully

This picture is transferred through mail to authorized person and again the authorized person can login and decrypt the browsed file through decryption key. The techniquesof encryption, data hiding and steganography in image. A new problem is trying to combine a single step, compression, encryption and data hiding [1,3]. So far, few solutions have been proposed to combine image encryption and compression 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 exist large variety of steganography techniques some are widely complex than others but all of them have respective strong and weak points, the first to employ hidden communications techniques because of the strategic importance to secure communication they need to conceal the source are 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 became very important these days, due to which around thirty of the major countries technologies in the world are using this methods and are discussing and analyzing the ratio based 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 proposing image encryption and for steganography to increase the security level of the encoded image and to make it less visible.

5. CONCLUSION

In this paper, one can see that there exists a large selection of approaches for hiding information in images. All the major image file formats have different methods of hiding messages, with different strong and weak points respectively. Image steganography technique was suggested here by splitting the long secret message into number of short segments. Then hide these short segments in different parts of the best matched in pixels of the segos image.

6. APPLICATION AREA

This steganography application software is provided for the purpose to use many type of images formats for hiding any type of files in side there [4].The master work of this application is in supporting pictures of any type without any need to convert to bitmap, and also to lower the limitation on file size to hide, because of using maximum memory space in pictures to hide the file.

7. FUTURE WORK

Future research by the author will involve detailed studies to investigate potential increased safety and ease of use benefits together with user acceptability.For a wide range of non-contact hand gesture human vehicle interaction applications.

REFERENCES

[1]N.F.Johnson, S.Jajodia, Exploring steganography: seeing the unseen, IEEE Computer 31 (2) (1998) 26–34.

[2]J.C.Judge, Steganography: past, present, future. SANS Institute publication, /http://www.sans.org/reading_room/whitepapers/ stenganography/552.phpS, 2001.

[3]N.Provos, P.Honeyman, Hide and seek: an introduction to steganography, IEEE SecurityandPrivacy1(3)(2003)32–44.

[4]P.Moulin, R.Koetter, Data hiding codes, Proceedings of th eIEEE93(12)(2005)2083–2126.

[5]S.B.Sadkhan, Cryptography: current status and future trends, in: Proceedings of IEEE International Conference on Information & Communication Technologies: From Theory to Applications, Da- mascus. Syria, April19–23,2004,pp.417–418.

[6]S.Lyu, H.Farid, Steganalysis using higher order image statistics, IEEE Transactions on Information Forensics and Security1 (1) (2006)111–119.

[7]Jamil, T., "Steganography: The art of hiding information is plain sight", IEEE Potentials, 18:01, 1999

[8] Wang, H & Wang, S, "Cyber warfare: Steganography vs.Steganalysis", Communications of the ACM,47:10, October 2004

[9]Adnan Gutub, Ayed Al-Qahtani, & Abdulaziz Tabakh. (2009). Triple-A: secure RGB image steganography based on randomization. AICCSA, IEEE/ACS International Conference on Computer Systems and Applications.

[10] W. Puec Image Encryption and Compression for Medical Image Security PROCEEDING OF IEEE Image Processing Theory, Tools & Applications.

[11] Ming YANG,Lei SONG,Monica TRIFAS,Dorothy BUENOS-AIRES,Lei CHEN, Jaleesa ELSTON,Secure Patient Information and Privacy in Medical Imaging IEEE.

[12] Xinpeng Zhang] ieee signal processing letters, VOL. 18, NO. 4, APRIL 2011 255 Reversible Data Hiding in Encrypted Image.

[13]X. Li, J. Wang, A steganographic method based upon JPEG and particle swarm optimization algorithm, Information Sciences 177 (15) (2007) 3099–31091.

[14]"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.

[15] "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.