A Novel Information Security Scheme using Cryptic Steganography

B.RAJA RAO
Associate Professor, E.C.E Dept
VKR & VNB Engineering College,
Gudivada, A.P, S.INDIA.
raja_rao_b@ yahoo.com

P.ANIL KUMAR
Assistant Professor, I.T Dept
VKR & VNB Engineering College,
Gudivada, A.P, S.INDIA.
anilkumar_pallikonda@yahoo.co.in

K RAMA MOHANA RAO
Assistant Professor, I.T Dept
VKR & VNB Engineering College,
Gudivada, A.P, S.INDIA.
raokmohan@yahoo.com

M.NAGU
Assistant Professor, E.C.E Dept
VKR & VNB Engineering College,
Gudivada, A.P, S.INDIA.
mng100174@gmail.com

Abstract:

The demand for effective information security schemes is increasing day by day with the exponential growth of Internet. Cryptography and Steganography are the two popular techniques for secret communication. The contents of message are kept secret in cryptography, where as in steganography the message is embedded into the cover image (text, video and image (pay load)).

In this proposed system we developed a system in which cryptography and steganography are used as integrated part along with newly developed enhanced security model. In cryptography we are using MD-5 Algorithm to encrypt a message and a part of message is hidden in DCT of an image, remaining part of the message is used to generate three (3) secret keys which make the system highly secured. To avoid the problem of unauthorized data access steganography along with cryptography called as Cryptic-Steganography scheme is the right most solution.

Key words:
Cryptography, steganography, encryption, decryption, Data security

1. INTRODUCTION

Steganography [1] is a data hiding technique that has been widely used in information security applications. It is similar to watermarking and cryptography techniques. However, these three techniques are different in some aspects.

1) Watermarking mainly prevents illegal copy or claims the ownership of digital media. It is not geared for communication.

2) Cryptography scrambles the data to be communicated so that unintended receivers cannot perceive the information. However, the fact that the communication has been carried out is known to everyone.

3) Steganography transmits data by embedding messages into innocuous-looking cover objects, such as digital images. As a result, the presence of communication is hidden. The choice of cover image is also important. Images with low number of colors, computer art, images with unique semantic content such as fonts should be avoided as cover images [2]

Cryptography and steganography are well known and widely used techniques that manipulate information in order to hide their existence respectively. Cryptography scrambles a message so it cannot be understood, where as the steganography hides the message so it cannot be seen. In this paper we focus to develop one system which uses both cryptography and steganography for high end security. The MD5 and LSB algorithms are very secured techniques for cryptography and steganography.

The basic design for the proposed technique is based on the idea:

- Scramble the message into encrypted text and hide a part of it.

- Unhidden part of the encrypted message will be converted into three (3) secret keys

To get the original text message one should know the 3 keys and the techniques implemented in cryptography and steganography.so the system becomes highly secured.

2. RELATED WORK

There are some specific security [3] requirements for cryptography including authentication, privacy and confidentiality .we have used MD5 algorithm [4] in cryptography.

MD5 is an algorithm that is used to verify data integrity through the creation of a 128-bit message digest from data input (which may be a message of any length) that is claimed to be as unique to that specific data as a fingerprint is to the specific individual. MD5, which was developed by Professor Ronald L. Rivest of MIT, is intended for use with digital signature applications, which require that large files must be compressed by a secure method before being encrypted with a secret key, under a public key cryptosystem.

Steganography is a tool to conceal high sensitive information and it is an art of hiding information in a plain sight. The word Steganography comes from the word steganos (covered) and graptos(writing)which technically means “covered or hidden writing ”.in ancient times messages were hidden on the back of wax writing tables, written on the stomachs of rabbits, or tattooed on the scalp of slaves. The majority of today’s steganographic systems uses multimedia objects like image, audio and video etc as cover media because people often transmit digital pictures over email and other internet communication. Depending upon the nature of cover object, steganography [5]can be divided into 5 types:

Text steganography, Image steganography, Audio steganography, video steganography, and Protocol steganography.Some of the steganography methods are

1. LSB
2. MASKING
3. FILTERING
4. TRANSFORM TECHNIQUE

The best known steganographic method that works in the spatial domain is the LSB (Least Significant Bit), which replaces the least significant bits of pixels selected to hide the information. A large number of commercial steganographic programs use the Least Significant Bit embedding (LSB) as the method of choice for message hiding in 24-bit, 8-bit color images, and grayscale images [6]. In this paper we have used lsb algorithm for steganography.

3. Proposed Technique

In this paper the problem of unauthorized data access is minimized by combining cryptography and steganography .In cryptography we have used md5 encryption algorithm and the ciper text is converted into three (3) keys for high security .then the LSB steganography is implemented to the key-2 to get stego image. The block diagram of the Cryptic-Steganography scheme is shown in figure 1.

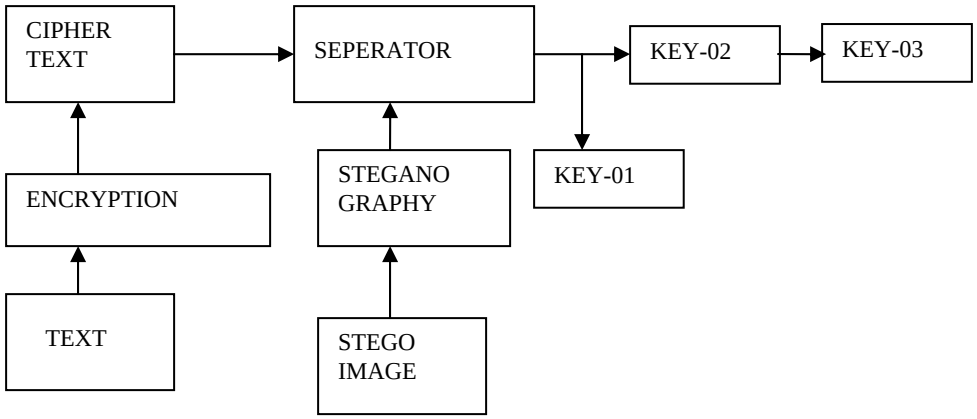


Fig.1: Block diagram of Cryptic-Steganography Scheme

3.1. Algorithm for hiding the text in proposed model:

1. Insert the text for Encryption.

2. Apply MD5 algorithm to get cipher text in hexadecimal form with Alphabets (A,B,C,D,E,F) and Digits 0 to 9.The cipher text is modified to generate 3 extra private keys

3. Separate the Alphabets and Digits from the cipher text by using separator.

4**. Key -1**: keep track of original position of alphabet and digits alternatively in the form of secret key -1 (if alphabets count is not equal to digits count, then write the larger in sequence at last)

6. **Key -2**: Separate first 10 alphabets retrieved from the step-3 and add the remaining alphabets at the end of separated digits to obtain key-2.

7. **key-3**: Take the Reversal of the key-2 to obtain key-3.

Hide the separated 10 alphabets by using least significant bit algorithm and find the Stego Image .

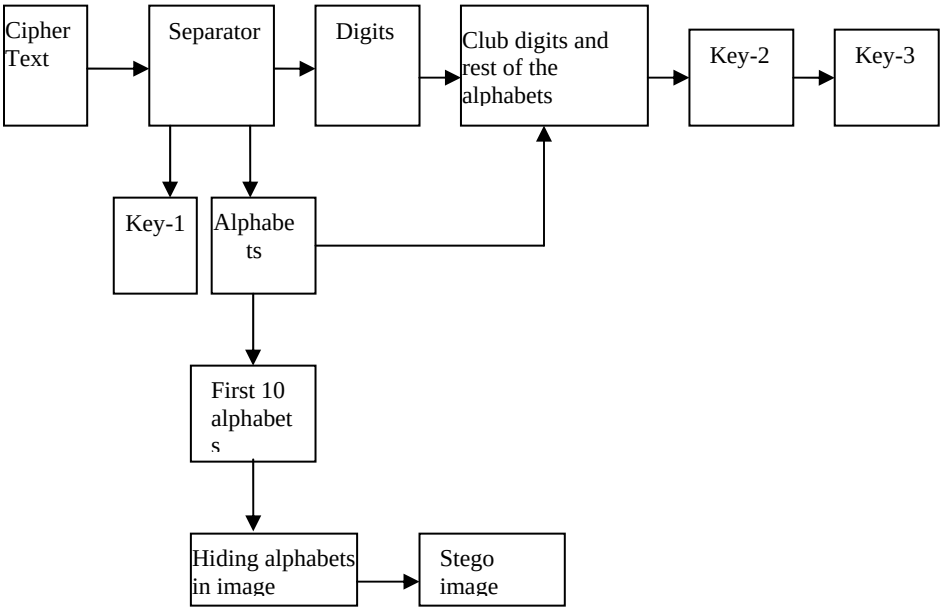


Fig.2: Block diagram for hiding the text in Cryptic-Steganography Scheme

3.2. Algorithm for Retrieving the text from the proposed model :

1. Retrieve the 10 characters from the Stego Image.

2. By key-3 obtain key-2 with reversing it.

3. Separate alphabets and digits from key-2.

4. Add back the rest of alphabets from key-2 to 10 characters of alphabets retrieved from image.

5. Find the alphabets and digits with the help of key 1 to get back the original cipher text in hexadecimal form.

6. Regenerate the original text message from the cipher text with the help of **MD5** decryption algorithm.

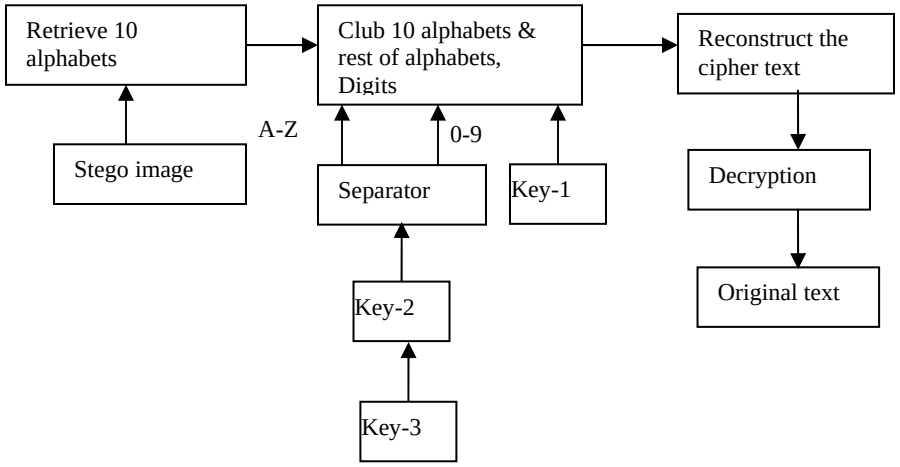


Fig.3: Block diagram for Retrieving the text in Cryptic-Steganography Scheme

The proposed solution is highly secure since
It's a combination of two highly secured techniques

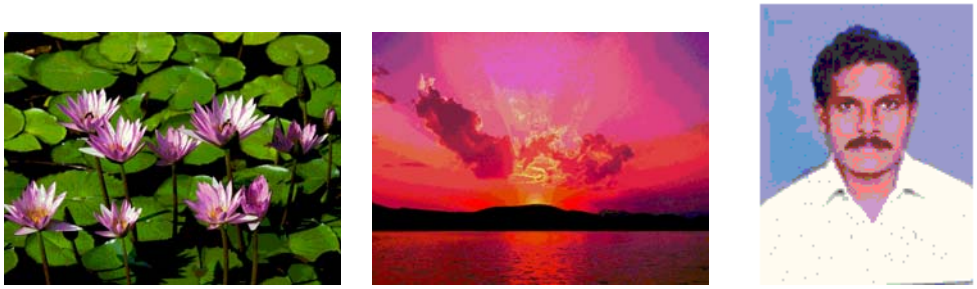
a) MD5 for cryptography
b) LSB and DCT manipulation for Steganography.

This system also contains total 4 keys.
a) One 128 bits private key for AES algorithm & 3 extra private generated keys for retrieving the original message.

The extra private keys make the system highly secured .If the intruder detect the partial part of the hidden message from the stego image it will be totally meaningless[7] .it is impossible to retrieve the original message until the complete set of keys are available.[8]

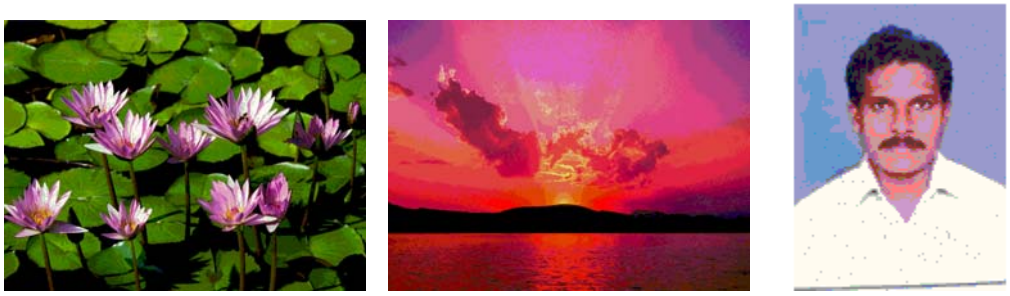
4. Results

The proposed High secured system using cryptography and steganography is tested by taking message and hiding them in some images of different sizes. The results that are obtained from these experiments are recorded and can be summarized in the following figures.



1.water lilies.bmp 2. sunset.bmp 3.photo.bmp

Fig.4: figures of cover images



1.water lilies.bmp 2. sunset.bmp 3.photo.bmp

Fig.5: figures of Stego images

The proposed Cryptic-Steganography system is tested by taking a message and hiding it in different images. The psnr is calculated for three different images. The results that are obtained from these experiments are summarized in table-1.

Table- 01: Experiments table

s.no	Image	psnr
01	Water lilies	51 . 9521
02	sunset	53. 5311
03	photo	57. 0209

5.Histogram analysis

The histograms of the cover and stego images are shown fig 6 .it clearly shows that the two histograms are identical. The effect is mainly due to the fact that the modifications are made at the DCT coefficients with large magnitudes which correspond to the noisy areas in original image.

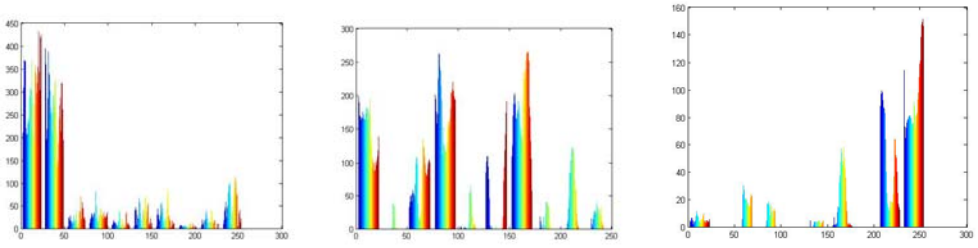


Fig .6: Histograms of cover images

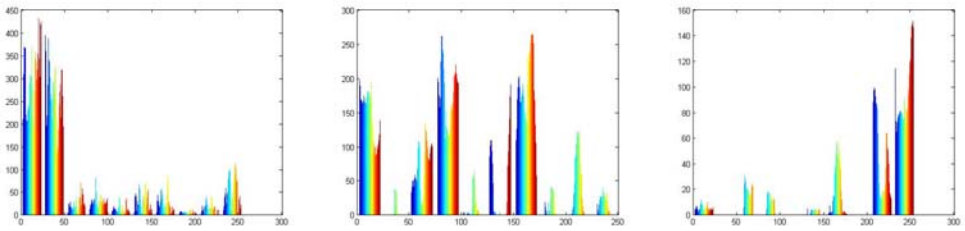


Fig .7: Histograms of Stego images

The proposed High secured system using cryptography and steganography is tested by taking message and hiding them in different images

6. CONCLUSION

The work accomplished during this paper can be summarized with the following points :In this paper we have presented a new system for the combination of cryptography and Steganography using three keys named as Cryptic-Steganography System which could be proven as a highly secured method for data communication in near future.

Steganography, especially combined with cryptography, is a powerful tool which enables people to communicate without possible eavesdroppers even knowing there is a form of communication in the first place. The proposed method provides acceptable image quality with very little distortion in the image.

The main advantage of this Cryptic-Steganography System is to provide high security for key information exchanging.

Cryptic-Steganography System find applications in medicine by doctors to combine explanatory information with in x-ray images. It is also useful in communications for codes self error correction. It can embed corrective audio or image data in case corruption occurs due to poor connection or transmission.

7. REFERENCES

[1] Domenico Daniele Bloisi , Luca Iocchi: Image based Steganography and cryptography, Computer Vision theory and applications volume 1 , pp. 127-134 .

[2].T.Aura .”an invisible communication”in proceedings of hut seminar on network security on network security.95.Espoo ,finland ,nov 1995.

[3] D.R. Stinson, Cryptography: Theory and Practice, BocaRaton, CRC Press, 1995.

[4]. Xiaoyun Wang; Hongbo Yu. "How to Break MD5 and Other Hash Functions". EUROCRYPT. ISBN 3-540-25910-4, 2005.

[5] .Chandramouli, R., Kharrazi, M. & Memon, N., “ImageSteganography and steganalysis: Concepts and Practice”,Proceedings of the 2nd International Workshop on DigitalWatermarking, October 2003.

[6]. J.Fridrich. M.goljan and R.Du .”distortion free data embedding for images “ proceedings .4 th information hiding workshop , Pittsburgh ,Pennsylvania,April 25-27,2001.

[7] Kharrazi, M., Sencar, H. T., and Memon, N. (2004). ImageSteganography: Concepts and practice. In WSPC LectureNotes Series

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

[09] Dunbar, B., “Steganography techniques and their use in an Open-Systems environment”, SANS Institute, January 2002