ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 2, April 2013

Secured Crypto-Stegano Communication through Unicode and Triple DES

Ms.M.Kavitha[1], Ms.S.Kawsalya[2]

Assistant professor, Department of Computer Applications,,Karpagam college of EngineeringCoimbatore,India[1]

HOD, Department of Software Systems, Kovai Kalaimagal College of Arts and Science,Coimbatore,India[2]

ABSTRACT*:* Cryptography is a way to provide security to the message which is passed between the sender and the receiver. It uses various algorithms to convert the actual message to an unreadable form. Steganography is an art of hiding the message in an medium. The medium can be audio, video, image or even a graph. It gives the security through the medium. The crypto-stegno communication uses both cryptography and steganography to send the message secretly from the sender to the receiver. This paper shows the usage of how message from sender is encrypted using triple DES through Unicode and hide the encrypted image into an stego image.. On the receiver end, extraction algorithm is designed in such a way that the process separates the message and image into two different entities; then reads the extracted message which is in the encrypted form and transforms it from the Unicode symbols to a readable form. The method is defined as undetectable, strong and secured communication of data related to the multimedia image. Thus any confidential message can be send to any target without the knowledge of others through an unsecured communication channel. This encoding and decoding scheme of the proposed new method is significantly different as compared to traditional schemes.

Keywords: Cryptanalysis, Mean Square Error, Peak Signal to Noise Ratio

I. INTRODUCTION

Cryptography is the art and science of protecting information from undesirable individuals by converting it into a form non-recognizable by its attackers while stored and transmitted [1]. Data cryptography mainly is the scrambling of the content of data, such as text, image, audio, video and so forth to make the data unreadable, invisible or unintelligible during transmission or storage called Encryption. The main goal of cryptography is keeping data secure form unauthorized attackers. The reverse of data encryption is data Decryption. In modern days cryptography is no longer limited to secure sensitive military information but recognized as one of the major components of the security policy of any organization and considered industry standard for providing information security, trust, controlling access to resources, and electronic financial transactions. There by which recuperate the original data.

II.STEGNOGRAPHY

Steganography is the art of hiding and transmitting data through apparently innocuous carriers in an effort to conceal the existence of the data, the word Steganography literally means covered or hiding writing as derived from Greek. Steganography has its place in security. It is not intended to replace cryptography but supplement it. Hiding a message with Steganography methods reduces the chance of a message being detected. If the message is also encrypted then it provides another layer of protection [1]. Therefore, some Steganographic methods combine traditional Cryptography with Steganography; the sender encrypts the secret message prior to the overall communication process, as it is more difficult for an attacker to detect embedded cipher text in a cover [32].

In the field of Steganography, some terminology has developed. The adjectives 'cover', 'embedded' and 'stego' were defined at the information hiding workshop held in Cambridge, England. The term "cover" refers to description of the original, innocent message, data, audio, video, and so on. Steganography is not a new science; it dates back to ancient times. It has been used through the ages by ordinary people, spies, rulers, government, and armies. There are many stories about Steganography. Information can be hidden in images [3], audio, video, text, or some other digitally representative code. Steganography systems can be grouped by the type of covers [5] used (graphics, sound, text, executables) or by the techniques used to modify the covers.

a. Substitution system [6].
b. Transform domain techniques [7]
c. Spread spectrum techniques
d. Statistical method[9]
e. Distortion techniques[14]

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 2, April 2013

f. Cover generation methods [14]

Thomas Jakobsen proposed [14] a method for fast cryptanalysis of substitution ciphers. This method explored the knowledge of diagram distribution and their mapping in the cipher text.

Recent approaches [14] in literature are being concentrated on retrieval of plain text, based on the features of the respective language. Certain language characteristics are to be identified for successful cryptanalysis. Extensive statistical analysis of frequency distribution of characters is an additive knowledge while retrieving part of plain text message.

Bárbara E. et al presented a method [14] for de-ciphering texts in Spanish using the probability of usage of letters in the language. The frequency of different letters is the clue to the presented de-ciphering. Bao-Chyuan et al proposed [14] a method to improve the encryption of oriental language texts with a case study on Chinese text files which are ideogram based and differ from Latin text. Moreover the number of characters that appear in Chinese are much larger when compared to English. The scheme proposed by Bao reported that large Chinese text can be handled more efficiently. A method for Parisian/Arabic script is proposed [15] with regard to shapes and their position in the word. The text Steganography methods that are especially designed for Persian and Arabic texts are surveyed.

In the Dot Steganography method [16], data is hidden in Persian and Arabic texts by using a special characteristic of these languages. Considering the existence of too many dots in Persian and Arabic characters, in this approach by vertical displacement of the dots by hiding information in the texts. This method does not attract attention and can hide a large volume of information in text.

The La Steganography method uses the special form of "La" word for hiding the data. This word is created by connecting "Lam" and "Alef" characters. For hiding bit 0, we use the normal form of word "La" (" ﻻ ") by inserting Arabic extension character between "Lam" and "Alef" characters. But for hiding bit 1, we use the special form of word "La" (" ﻵ") which has a unique code in the Unicode Standard (its code is FEFB in Unicode hex notation). This method is not limited to electronic documents (e-documents) and can also be used on printed documents.

There have been several successful attempts to design text steganography based on the characteristic of their features, for example in these languages; English [18]-[21], Japanese [22], Korean [23], Chinese [24]-[25], Arabic [26].

The Shirali-Shahreza's [27] methods hide the secret information in the points (dots) location within the pointed (dots) letters. The length of the secret information is identified (example 20 bits) and compress. The cover medium text is scanned line by line, character by character. Whenever a pointed (dots) letter is detected, its points (dots) location may be affected by the hidden information bit. If the hidden bit is one, the point (dot) is slightly shifted up; otherwise the concerned cover-text character point location remains unchanged.

The Kashidah method proposed by Adnan [28] exploits the existence of the redundant Arabic extension character (Kashidah) and the pointed (dots) letters. This method is more practical: the pointed letters with a Kashidah will hold the secret bit "1" and the unpointed (without dots) letters with a Kashidah to hold "0". The character extension has a standard character hexadecimal code of 0640 in Unicode system and this method does not have any effect to the writing content.

The La Steganography method [27] uses a special form of La word (a combination of the Lam and Alef caharacters) for hiding the data, i.e. by inserting an Arabic extension character between the Lam and Alef. For hiding bit 0, they use the normal form of La, whereas bit 1 is hidden using the special word La with a unique code in the Standard Unicode (i.e. FEFB in the Unicode hex notation).

The method [29], uses the pointed letters with extension (Kashida in Arabic) to hold secret bit 'one' and the un-pointed letters with extension to hold secret bit 'zero'. Note that letter extension does not have any effect to the writing content. It has a standard character hexadecimal code of 0640 in the Unicode system.

For example ancient Greece used methods for hiding messages such as hiding it in the belly of a share (a kind of rabbits), using invisible ink and pigeons. Another ingenious method was to shave the head of a messenger and tattoo a message or image on the messenger head. After allowing his hair to grow, the message would be undetected until the head was shaved again. While the Egyptian used illustrations to conceal message. Hidden information in the cover data is known as the "embedded" data and Unicode hiding is a general term encompassing many sub disciplines, is a term around a wide range of problems beyond that of embedding message in content. The term hiding here can refer to either making the information undetectable or keeping the existence of the information secret. Information hiding is a technique of hiding secret using redundant cover data such as images, audios, movies, documents, etc. This technique has recently become important in a number of application areas. For example, digital video, audio, and images are increasingly embedded with imperceptible marks, which may contain hidden signatures or watermarks that help to prevent unauthorized copy. It is a performance that inserts secret messages into a cover file, so that the existence of the messages is not apparent.

III. CRYPTO-STEGNOGRAPHY

The crypto-stegno communication uses both cryptography and stegnography to send the message secretly from the sender to the receiver.This paper shows the usage of how message from sender is encrypted using triple DES

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 2, April 2013

through Unicode and hide the encrypted image into an stego image.. On the receiver end, extraction algorithm is designed in such a way that the process separates the message and image into two different entities; then reads the extracted message which is in the encrypted form and transforms it from the Unicode symbols to a readable form.

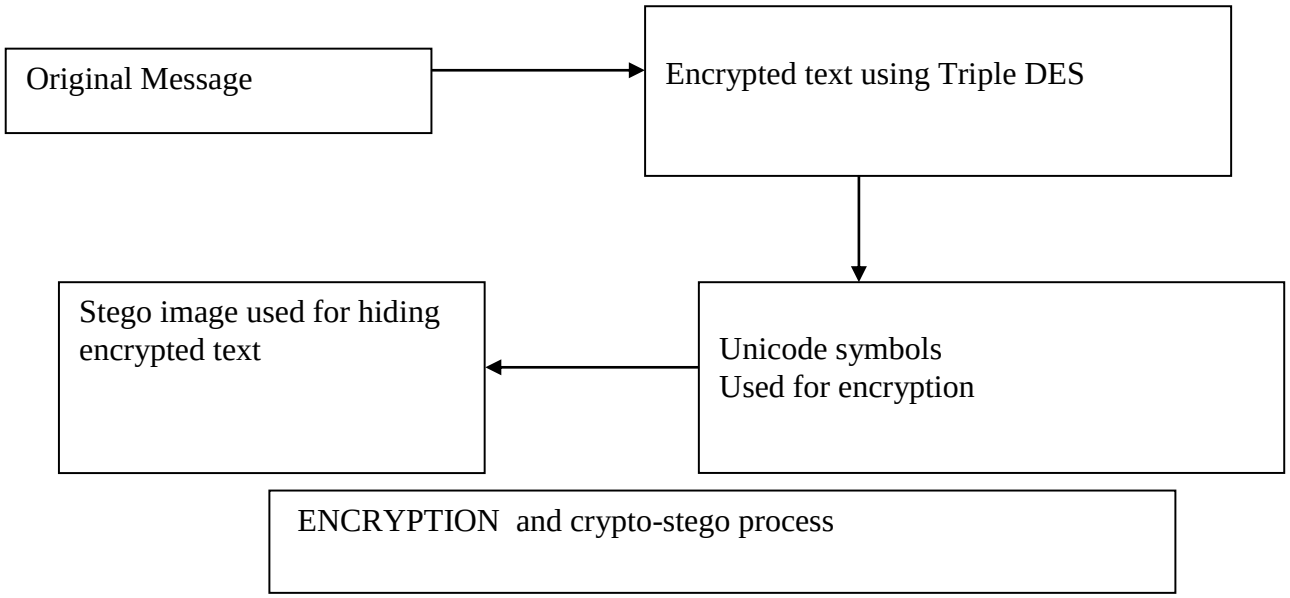

Figure 1.Encryption

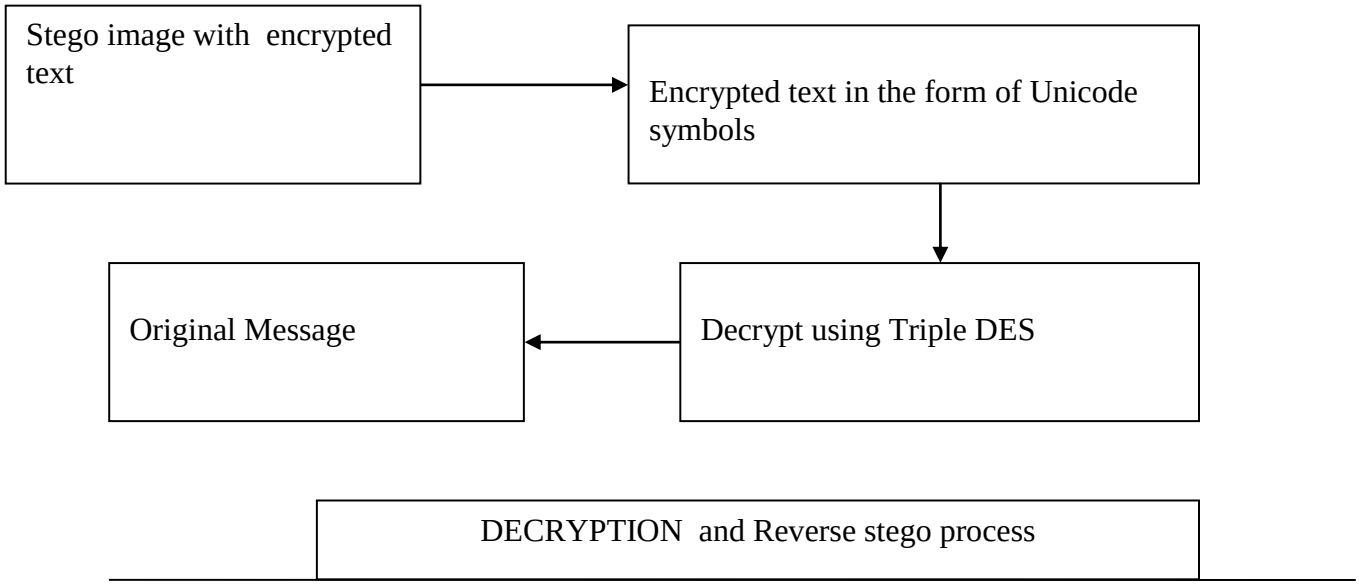

Fig.2. Decryption

IV. IMPLEMENTATAION IN MATLAB

MATLAB (**mat**rix **lab**oratory) is a numerical computing environment and fourth-generation programming language. Developed by MathWorks, MATLAB allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs written in other languages, including C, C++, Java, and Fortran Cleve Moler, the chairman of the computer-science department at the University of New Mexico started developing MATLAB in the late 1970s He designed it to give his students access to LINPACK and EISPACK without them having to learn Fortran.

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 2, April 2013

It soon spread to other universities and found a strong audience within the applied mathematics community. Jack Little, an engineer, was exposed to it during a visit Moler made to Stanford University in 1983. Recognizing its commercial potential, he joined with Moler and Steve Bangert. They rewrote MATLAB in C and founded MathWorks in 1984 to continue its development. These rewritten libraries were known as JACKPAC In 2000, MATLAB was rewritten to use a newer set of libraries for matrix manipulation, LAPACK MATLAB was first adopted by researchers and practitioners in control engineering, Little's specialty, but quickly spread to many other domains. It is now also used in education, in particular the teaching of linear algebra and numerical analysis, and is popular amongst scientists involved in image processing.

V.UNICODE

UNICODE is a computing industry standard for the consistent representation and handling of text expressed in most of the world's writing systems. Developed in conjunction with the Universal Character Set standard and published in book form as The UNICODE Standard, the latest version of UNICODE consists of a repertoire of more than 107,000 characters covering 90 scripts, a set of code charts for visual reference, an encoding methodology and set of standard character encodings, an enumeration of character properties such as upper and lower case, a set of reference data computer files, and a number of related items, such as character properties, rules for normalization, decomposition collation, rendering, and bidirectional display order (for the correct display of text containing both right to -left scripts, such as Arabic or Hebrew, and left-to-right scripts).

The objective of UNICODE is to unify all the different encoding schemes so that the confusion between computers can be limited as much as possible. It has several character encoding forms, UTF standing for UNICODE Transformation Unit:

- UTF-8: only uses one byte (8 bits) to encode English characters. It can use a sequence of bytes to encode the other characters. UTF-8 is widely used in email systems and on the Internet.
- UTF-16: uses two bytes (16 bits) to encode the most commonly used characters. If needed, the additional characters can be represented by a pair of 16-bit numbers.
- UTF-32: uses four bytes (32 bits) to encode the characters. It became apparent that as the UNICODE standard grew a 16-bit number is too small to represent all the characters. UTF-32 is capable of representing every UNICODE character as one number.

VI.TRIPLE DES

TripleDES with three different keys (K1, K2 and K3) has effective key length is 168 bits (The use of three distinct key is recommended of TripleDES.). Another variation is called two-key (K1 and K3 is same) TripleDES reduces the effective key size to 112 bits which is less secure. Two-key TripleDES is widely used in electronic payments industry. TripleDES takes three times as much CPU power than compare with its predecessor which is significant performance hit.

The TripleDES evaluation criteria among DES was done using

- Security
- Software & Hardware performance
- Possible Keys
- Resistance to power analysis and other implementation attacks.
- Printable key characters

By design TripleDES is faster in software and works efficiently in hardware. It works fast even on small devices such as smart phones; smart cards etc. The TripleDES provides more security due to larger block size and longer keys.

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 2, April 2013

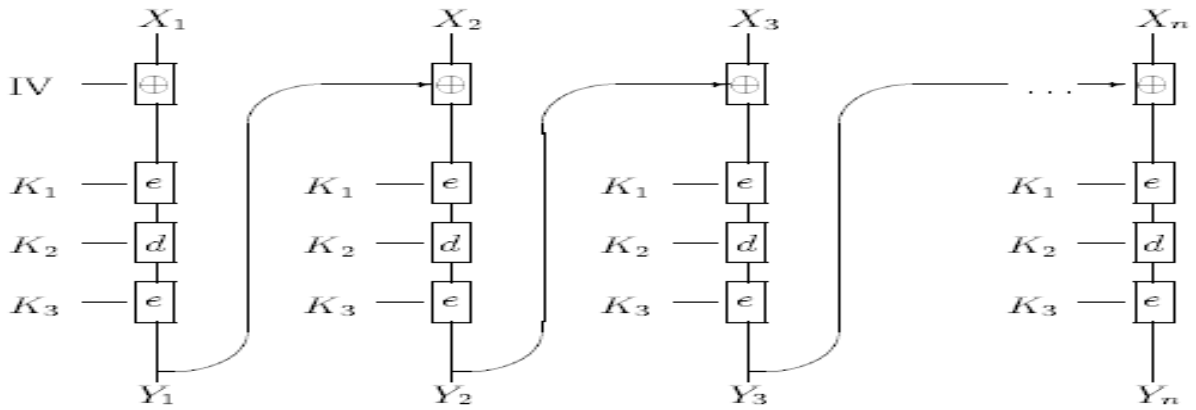

Figure 3. Triple DES

The encryption algorithm is:
ciphertext = EK3(DK2(EK1(plaintext)))
I.e., DES encrypt with K1, DES decrypt with K2, then DES encrypt with K3.
Decryption is the reverse:
plaintext = DK1(EK2(DK3(ciphertext)))
I.e., decrypt with K3, encrypt with K2, then decrypt with K1.Each triple encryption encrypts one block of 64 bits of data.In each case the middle operation is the reverse of the first and last. This improves the strength of the algorithm when using keying option 2, and provides backward compatibility with DES with keying option 3.
Keying options
The standards define three keying options:
Keying option 1: All three keys are independent.
Keying option 2: K1 and K2 are independent, and K3 = K1.
Keying option 3: All three keys are identical, i.e. K1 = K2 = K3.
Keying option 1 is the strongest, with 3 × 56 = 168 independent key bits.Keying option 2 provides less security, with 2 × 56 = 112 key bits. This option is stronger than simply DES encrypting twice, e.g. with K1 and K2, because it protects againstmeet-in-the-middle attacks. Keying option 3 is equivalent to DES, with only 56 key bits. This option provides backward compatibility with DES, because the first and second DES operations cancel out. It is no longer recommended by the National Institute of Standards and Technology (NIST) and is not supported by ISO/IEC 18033-3.
Other terms used to refer to the keying options
"Keying option n" is the term used by the standards (X9.52, FIPS PUB 46-3, SP 800-67, ISO/IEC 18033-3) that define the TDEA. However, other terms are used in other standards and related recommendations, and general usage.
For keying option 1:
3TDEA, in NIST SP 800-57 and SP 800-78-3Triple-length keys, in general usage
For keying option 2:
2TDEA, in NIST SP 800-57 and SP 800-78-3 Double-length keys, in general usage

VII. ALGORITHM

Generating Unicode symbols and hiding message
Input: Secret Message and an image
Output: Crypto-Stegano object contains image as carrier text is compressed using runlength encoding with Unicode symbols.
Steps:
1. Input the secret message to be hidden
2. Extract each character from the message
3. Encrypt the message using triple DES(use Key1,2,3).
4. Embed the character in Unicode format
5. Display the equivalent Unicode symbol
6. Repeat the process until all characters are converted into Unicode symbols
7. Compress the content to reduce the size of the file
9. Select an image as carrier to hide the file

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 2, April 2013

Message Extraction
Input: Crypto-Stegano object
Output : Secret message in readable form
Steps:
1. Select the crypto-stegano object
2. Discover the keys for triple DES
3. Extract the compressed file from the crypto-stegano object
4. Convert the compressed content to a normal content
5. Read each Unicode symbol from the text file
6. For each Unicode symbol find the equivalent characters.
7. Repeat step 5 and 6 until all the Unicode symbols are converted into characters
8. Accumulated characters form the secret message

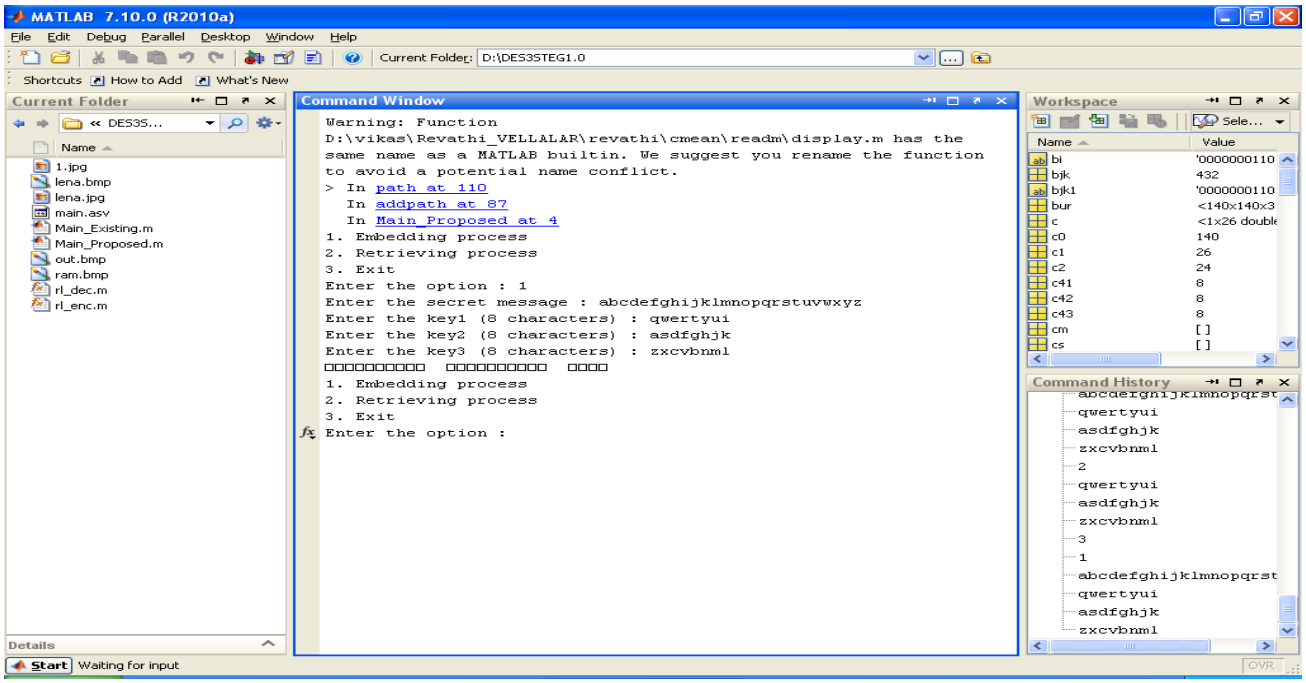

Figure 4.Encryption Process

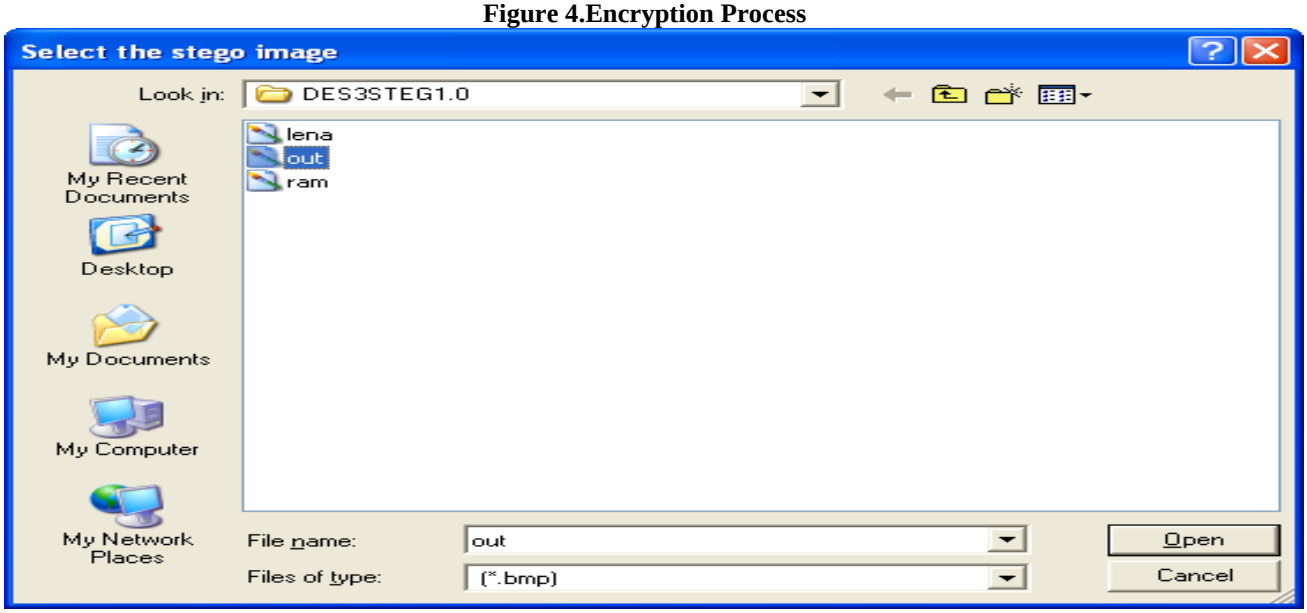

Figure 5. Selection of Stego image

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 2, April 2013

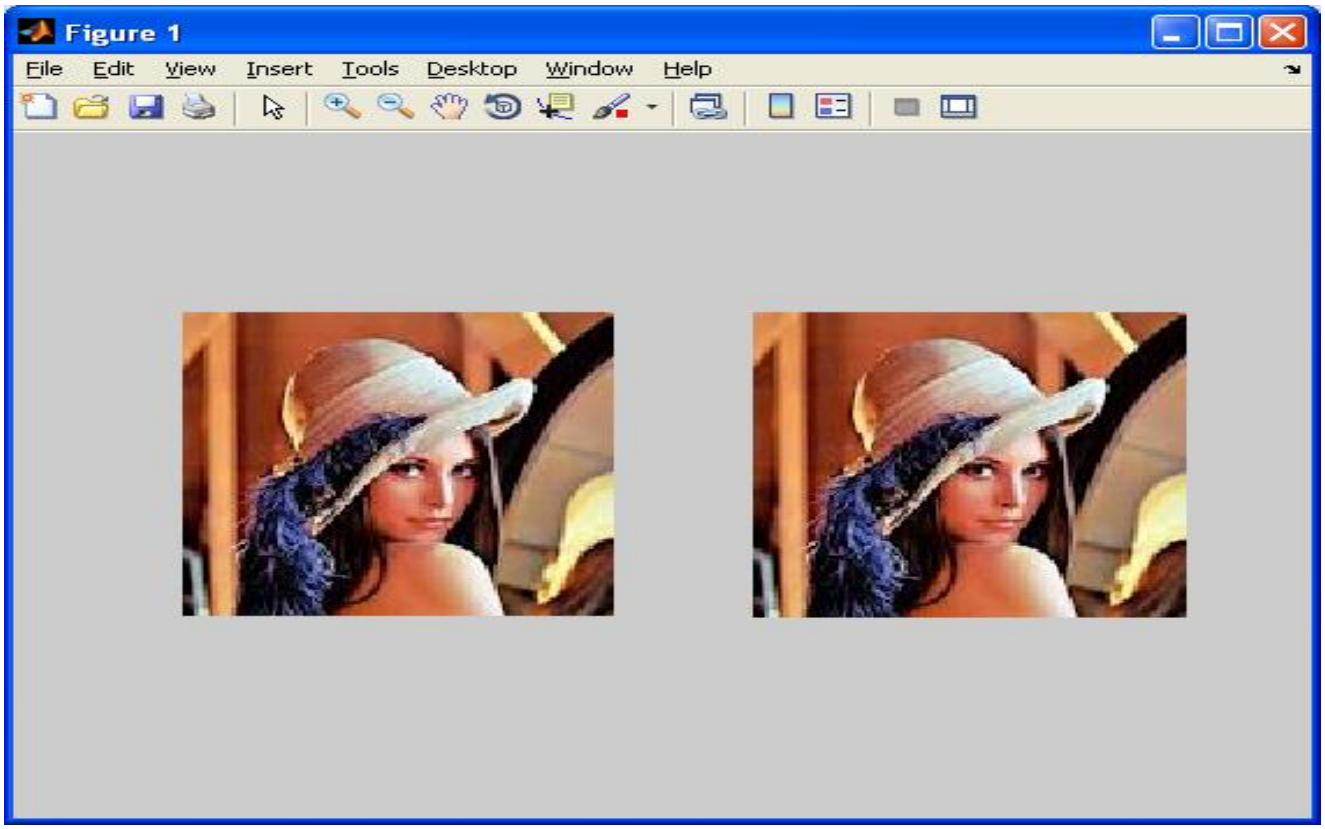

Figure 6: Output of the Image Using Triple-DES

VIII. EVALUATION ANALYSIS

To evaluate the performance of proposed method it need to compare with the existing one

A. Key Length

The key length is an important security parameter in cryptographic function. The key length is measured in bits.For TripleDES the key length is to be 168 bits (K_1, K_2, K_3), here the K_1, K_2 are same so the key length of the TripleDES is 112 bits. Due to high key length the security of the system is increased. Whereas the DES system which as only 56 bits.

B. Cryptanalysis Resistance Security

The Cryptanalysis Resistance Security is given some encrypted data that is ciphertext, the goal of the cryptanalyst is to gain as much information as possible about the original, unencrypted data called plaintext.

In proposed method the resistance is vulnerable to differential cryptanalysis. In which the brute force attackers could be analyze the plain text using differential cryptanalysis. As in DES it is weak to analyze the plain text.

C. Possible Keys

The possible keys for the TripleDES are 2^{112} or 2^{168}. Were as the possible keys for DES is 2^{56}.

D. Possible ASCII Printable Character Keys

In proposed method the possible ASCII Printable Character Keys are 95^{14} or 95^{21}. Were as in the existing method the ASCII Printable Character Key is 95^{7}. Due to the large number of keys we can print the large number of characters.

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 2, April 2013

	Triple DES	DES
Key Length	168 bits	56 bits
Cryptanalysis Resistance Security	Efficient in Analyze the Plain Text	Weak in Analyze the Plain Text
Possible Keys	2^{112} or 2^{168}	2^{56}
Possible ASCII Printable Character Keys	95^{14} or 95^{21}	95^{7}

Table 1.Comparison of DES and Triple DES

From the above Table 1 the proposed Triple DES is more efficient and encrypt the high number of data's as compared with the existing DES. Hence the security level is strong as compared with the existing one.

IX. IMAGE QUALITY ANALYSIS

The Image Quality Analysis is done through by calculating the PSNR and the MSE Values. The PSNR block computes the peak signal-to-noise ratio, in decibels, between two images. This ratio is often used as a quality measurement between the original and a compressed image. The higher the PSNR, the better the quality of the compressed, or reconstructed image.

The *Mean Square Error (MSE)* and the *Peak Signal to Noise Ratio (PSNR)* are the two error metrics used to compare image compression quality. The MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error. The lower the value of MSE, the lower the error.

To compute the PSNR, the block first calculates the mean-squared error using the following equation:

$$MSE = \frac{\sum_{M,N} [I_1(m,n) - I_2(m,n)]^2}{M * N}$$

In the previous equation, *M* and *N* are the number of rows and columns in the input images, respectively. Then the block computes the PSNR using the following equation:

$$PSNR = 10 \log_{10} \left(\frac{R^2}{MSE} \right)$$

In the previous equation, *R* is the maximum fluctuation in the input image data type. For example, if the input image has a double-precision floating-point data type, then *R* is 1. If it has an 8-bit unsigned integer data type, *R* is 255, etc.where and denote the original and the encoded pixel values and is the total number of pixels in an image.

Various Methods	PSNR Values	MSE Values
DES Method	50.12	25.98
Triple DES Method	54.70	21.75

Table 2. Image Quality Analysis

From the above Table 2 we came to know that the proposed method of Triple-DES having the high PSNR values and the low MSE values as compared with the existing DES method. This work presents a scheme that can transmit large quantities of secret information and provide secure communication between two parties. Steganography with cryptographic password can be woven into this scheme to make the detection more complicated. Any kind of text data can be employed as secret message and is sent over the open channel. In addition, the proposed procedure is simple and easy to implement.

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 2, April 2013

X. CONCLUSION AND FUTURE WORK

As cryptography and steganography becomes more widely used in computing, there are issues that need to be resolved. There are a wide variety of different techniques with their own advantages and disadvantages. Many currently used techniques are not robust enough to prevent detection and removal of embedded data. The use of benchmarking to evaluate techniques should become more common and a more standard definition of robustness is required to help overcome this. For a system to be considered as robust it should have the following properties [2] such as (i) the quality of the carrier should not visibly degrade upon addition of a secret message (ii) secret message should be undetectable without secret knowledge, typically the key (iii) the secret data should survive attacks that don't degrade the perceived quality of the work.

Most of the steganographic techniques available today use the pixel bits of an image to hide information and are limited in terms of information hiding capacity. Small piece of information can only be embedded in an image carrier because of the limitation of altering more pixels which reduces the intensity of the image and create suspicion to others when passing through an open channel. In the proposed method, since information is stored in a text file and hidden in an image, its hiding capacity can be as large as a message to be conveyed in secret. This method produces a high strong security to transmit the text file in hidden format.

Triple DES was the answer to many of the shortcomings of DES. Since it is based on the DES algorithm, it is very easy to modify existing software to use Triple DES. It also has the advantage of proven reliability and a longer key length that eliminates many of the shortcut attacks that can be used to reduce the amount of time it takes to break DES. However, even this more powerful version of DES may not be strong enough to protect data for very much longer. The DES algorithm itself has become obsolete and is in need of replacement. To this end the National Institute of Standards and Technology (NIST) is holding a competition to develop the Triple DES as a replacement for DES. This is chiefly due to the 56-bit key size being too small as compared with the proposed one. There are also some analytical results which demonstrate theoretical weaknesses in the cipher, although they are infeasible to mount in practice. So the Triple-DES algorithm is believed to be practically secure even there are theoretical attacks. In future the National Institute of Standards and Technology (NIST) is holding a competition to develop the Advanced Encryption Standard (AES) algorithm as a replacement for Triple DES.

REFERENCES

1. B.B.Zaidan, A.A. Zaidan, A.K. Al-Frajat and H.A. Jalab,"On the Differences between Hiding Information and Cryptography Techniques: An Overview", Journal of Applied Sciences,Vol.10, pp.1650-1655,2010.
2. Domenico Daniele Bloisi , Luca Iocchi: Image based Steganography and cryptography, Computer Vision theory and applications Vol.1 , pp. 127-134,2007
3. Chandramouli, R., Kharrazi, M. & Memon, N., "Image Steganography and steganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking,Vol.1,pp.35-49,2003
4. Owens, M., "A discussion of covert channels and steganography", SANS Institute, Vol.1,pp.1-18, 2002
5. Jamil, T., "Steganography: The art of hiding information is plain sight", IEEE Potentials, Vol.1,pp.1-18,1999
6. Stefan Katznbeisser, Fabien.A., P.Petitcolas editors, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Boston. London,Vol.4,pp.36-42, 2012.
7. Marvel, L.M., Boncelet Jr., C.G. & Retter, C., "Spread Spectrum Steganography", IEEE Transactions on image processing, Vol.4, pp.8, 1999.
8. Bender, W., Gruhl, D., Morimoto, N. & Lu, A., "Techniques for data hiding", IBM Systems Journal, Vol 35, pp.3-4, 1996
9. Jakobsen, T., "A fast Method for Cryptanalysis of Subsittution Ciphers". Cryptologia, XIX, Vol.3, pp.265-274, 1995.
10. Majdi Al-qdah & Lin Yi Hui "Simple Encryption/Decryption Application" International Journal of Computer Science and Security, Vol.1, pp.1-20, 2007.
11. Bárbara E. Sánchez Rinza, Diana Alejandra Bigurra Zavala, Alonso Corona Chavez, "Deencryption of a text in spanish using probability and statistics" In the Proceedings of the 18th IEEE Conference on Electronics, Communications and Computers,pp 75-77, 2008.
12. Bao-Chyuan Guan; Ray-I Chang; Yung Chung Wei; Chia-Ling Hu; Yu-Lin Chiu, "An encryption scheme for large Chinese texts" , In Proceedings of the IEEE 37th Annual 2003 International Carnahan Conference on Security Technology , Taipei, Taiwan, ROC, pp 564- 568, 2003.
13. M.H. Shirali-Shahreza , M. Shirali-Shahreza, "Steganography in Persian and Arabic UnicodeTexts Using Pseudo-Space and Pseudo-Connection Characters". Theoretical and Applied Information Technology (JATIT).Vol.4, pp 682-687, 2008
14. M.H. Shirali-Shahreza and M. Shirali-Shahreza, "A New Approach to Persian/Arabic Text Steganography", Proceedings of the 5th IEEE/ACIS International Conference on Computer and Information Science (ICIS 2006), Honolulu, HI, USA, pp. 310- 315, 2006.
18. J. T. Brassil, S. Low, and N. F. Maxemchuk, "Copyright protection for the electronic distribution of text documents," Proceedings of the IEEE, Vol. 87, pp. 1181–1196, 1999.
19. D. Huang and H. Yan, "Interword distance changes represented by sine waves for watermarking text images," IEEE Transactions on Circuits and Systems for Video Technology, Vol. 11, pp. 1237– 1245, 2001.
20. Y.-W. Kim, K.-A. Moon, and I.-S. Oh, "A text watermarking algorithm based on word classification and inter-word space statistics," Proceedings of the Seventh International Conference on Document Analysis and Recognition, pp. 775–779, 2003.
21. M. Topkara, C. M. Taskiran, and E. J. Delp, "Natural language watermarking," in Proceedings of SPIE-IS & T Electronic Imaging,Vol.1, pp.441-452, 2005.

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 2, April 2013

22. T. Amano and D. Misaki, "A feature calibration method for watermarking of document images," in Proceedings of the Fifth International Conference on Document Analysis and Recognition ICDAR'99, September 1999, pp. 91–94,1999
23. Y.-W. Kim and I.-S. Oh, "Watermarking Text document images using edge direction histograms,"Pattern Recognition Letters, Vol. 25, pp. 1243–1251, 2004.
24. X. Sun, G. Luo, and H. Huang, "Componentbased digital watermarking of Chinese texts,"in Proceedings of the 3rd International Conference on information security, Shanghai, China,Vol.1, pp. 76–81, 2004
25. W. Zhang, Z. Zeng, G. Pu, and H. Zhu, "Chinese text watermarking based on occlusive components," The 2nd Information and communication Texhnology ICTTA'06, Vol. 1, pp.1850–1854, 2006.
26. M. Shirali- Shahreza,"A New Approach to Persian/Arabic Text Steganography", Proceedings of the 5th IEEE/ACIS International Conference on Computer and Information Science (ICIS 2006),Honolulu, HI, USA, pp. 310-315, 2006
27. M. Shirali-Shahreza, "A New Persian/Arabic Text Steganography Using "La" Word", Proceedings of the International Joint Conference on Computer, Information, and Systems Sciences, and Engineering (CISSE2007), Bridgeport, CT, USA,Vol.2,pp.339-342, 2007.
28. A. Gutub and M. Fattani, "A Novel Arabic Text Steganography Method Using Letter Points and Extensions", Proceedings of the WASET International Conference on Computer,Information and Systems Science and Engineering (ICCISSE), Vienna, Austria, Vol.21, pp. 28-31, 2007.
29. A. Gutub and M. Fattani, "A Novel Arabic Text Steganography Method Using Letter Points and Extensions", Proceedings of the WASET International Conference on Computer, Information and Systems Science and Engineering (ICCISSE), Vienna, Austria, Vol. 21, pp. 28-31, 2007
30. A.A.Zaidan, Fazidah. Othman, B.B.Zaidan, R.Z.Raji, Ahmed.K.Hasan, and A.W.Naji," Securing Cover-File without Limitation of Hidden Data Size Using Computation between Cryptography and Steganography ", World Congress on Engineering 2009 (WCE), Vol.1, p.p259-265,2009.
31. A.A.Zaidan, A.W. Naji, Shihab A. Hameed, Fazidah Othman and B.B. Zaidan, " Approved Undetectable-Antivirus Steganography for Multimedia Information in PE-File ",International Conference on IACSIT Spring Conference (IACSIT-SC09) , Advanced Management Science (AMS), Vol 1,p.p 425-429, 2009
32. B.B Zaidan, A.A Zaidan, Fazidah Othman, R.Z.Raji, S.M.Mohammed, M.M.Abdulrazzaq, "Quality of Image vs. Quantity of Data Hidden in the Image", International Conference on Image Processing, Computer Vision, and Pattern Recognition (IPCV'09), pp.345-350, 2009,
33. A. W. Naji, Shihab A. Hameed, Md Rafiqul Islam, B. B. Zaidan,Teddy S. Gunawan, and A. A. Zaidan," "Stego-Analysis Chain," vol.1, pp. 398-401 , 2009