ISSN:0975-9646

An Innovative Data Security Techniques Using Cryptography and Steganographic Techniques

Richa Dubey, Apurva Saxena, Sunita Gond
Assistant Professor, BUIT Barkatullah University Bhopal

Abstract- Intenet is now a day used to communicate and transferred all the information through insecure medium. There are number of malicious users try to hack the information. To keep the information secure various techniques are used. There are two type of cryptographic algorithm used: encryption/decryption algorithm and steganography algorithm. Steganography is the process of exchanging top secret information in a manner that nobody else can detect the presence of that secret message. For higher security steganography algorithm is used to combine with encryption/decryption algorithm. Many techniques have studied for steganography algorithms, but in this paper a new combine technique of cryptanalysis and steganalysis using HTML file is used. RJDA is a technique which uses LSB (least significant bit) as steganographic algorithm and encryption/decryption algorithm. Confidentiality is one of the most important parameter in security to ensure that no other unauthenticated person can understand the meaning of save or transmitted data. This paper proposed a new way of steganography which hided the data behind the HTML file with a reduced cover size than the existing one.

Keywords-Computer Security, Network, Encryption/Decryption Algorithm, Cryptography, Symmetric Key Algorithm, Steganography.

I. INTRODUCTION

As the development of Internet technologies increases, the transmission of digital media is now-a-days convenient over the networks

Data and information security keeps most importance in today's fast developing era. Various networks are used to exchange the information, which may be secure or sometime not secure. With the rapid growth of computer networks and advancement in technology, a large amount of information is being exchanged. Most of the information is confidential or private which increases the demand for stronger encryption techniques. Security has become a critical feature for capable networks. Communication is not safe due to the presence of some malicious users who wait for a chance to gain access to confidential data. Cryptography is derived from the Greek words "kryptos" (meaning "hidden") and "graphein" (meaning "to write"). Cryptography is the study of shuffling information in such a way that no one can understand the original meaning of message without knowing the secret key which make it again original text. The process of converting information (plain text) by transforming it into unreadable format (cipher text) is known as encryption. Encryption techniques can be sometimes broken by cryptanalysis, also called as code breaking, although modern cryptographic techniques are virtually unbreakable. Cryptography encrypts the original message that is being sent. This mechanism employs mathematical schemes and algorithms to scramble data into unreadable format. It can only be decoded or decrypted by the party that possesses the associated key [5]. Steganography is derived from the Greek word "stegnos" (meaning "covered/secret") and "graphein" (meaning "to write/draw") [2]. Steganography is the study of means of hiding the information in order to prevent hackers from detecting the presence of the secret information. The process of hiding the message in a cover without leaving a remarkable trace is known as Steganography. Steganography is the form of convert communication in which a secret message is hided with a carrier data. Steganography facade the presence of communication, making the true message not easily observable by the observer. Cryptography and Steganography achieve the same goal using different means. Encryption encodes the data so that an unintended recipient cannot determine its intended meaning. Steganography in contrast attempts to prevent an unintended recipient from suspecting that the data is there [3]. The authors studied both the algorithms and studied the techniques that use both the algorithm to provide high degree of security and also compare the result on the basis of timing and avalanche effect.

II. LITERATURE SURVEY

There are many algorithms which are proposed in the past, which used image file in steganalysis, between all the algorithms LSB is considered as the superior technique among all competitive ones, since it has very low noise of the cover file.

Deyan Chen [18] provides a concise but all-round analysis on data security and privacy protection issues associated with cloud computing across all stages of data life cycle. Then this paper discusses some current solutions. Finally, this paper describes future research work about data security and privacy protection issues in cloud.

Lukas Malina and Jan Hajny [19] present a novel privacy-preserving security solution for cloud services. They deal with user anonymous access to cloud services and shared storage servers. Solution

provides registered users anonymous access to cloud services. Users can use services without any threat of profiling their behaviour. They analyze current privacy preserving solutions for cloud services and outline the solution based on advanced cryptographic components.

Rishav Ray, Jeeyan Sanyal, Debanjan Das, Asoke Nath[1] propose a technique which shows the use of text file/MS word file as a cover file to hide the secret data. To increase

the degree of security authors have first encrypted the secret data by using Modified Generalized Vernam Cipher Method (MGVCM) and then hide the encrypted text behind the text file. Authors have proposed two new algorithms one is encryption/decryption algorithm and second algorithm is the hiding algorithm which explained the method to hide the secret message behind the text file. Authors have named his proposed algorithm "RJDA" which is architecture of joining these proposed two algorithms. The secret message comprising bits are inserted in place of 8 randomly selected blank spaces in the cover file. For this the secret message is first converted into binary format, where each character is represented by 8 bits. To hide each bit they have used blank spaces and also to hide bit 0 they have left the blank space as it is, and for bit 1 the blank space is replaced by a character having ASCII value 160 which also appears as a blank space on printing.

Meheboob Alam Mallik, Saima Gosh, Ashok Nath,Joyshree Nath[3]shows development of a new technique in which the encrypted message is hide behind the image cover file by substituting in 4^{th} bit position. LSB for encryption and they have used a new algorithm called MSA for hiding. They have 2 distinct algorithms (i) to encrypt secret message(SM) using MSA(Meheboob,Saima and Asoke) proposed by Nath et al.(1). (ii) they insert the encrypted secret message inside the cover file(CF) by changing the 4-th bit from the least significant bit(LSB).

Nath et al(2) already proposed different methods for embedding SM into CF but there the SF was inserted as it is in the CF and hence the security of steganography was not very high. In the present work they have basically tried to make the steganography method more secured. One can extract SM from CF but cannot be decrypted as one has to execute the exact decryption method. In present work they try to embed almost any type of file inside some standard cover file (CF) such as image file (.JPEG or .BMP) or any image file inside another image file. In this method the steganographic technique is first depicted for including different type of files with any type of file and they will describe the encryption technique to encrypt and decrypt the secret text.

Manoj Kumar Ramaiya,Naveen Hemrajani and Anil Kishore saxena[4] description discovers a unique technique for Image steganography which brings the use of Data Encryption Standard (DES) power of S- Box mapping & Secret key. Embedding function of the steganography algorithm using two unique S-boxes is used in the algorithm. The pre-processing of secrete image is done. The pre-processing provide high level of security as extraction is not possible without the knowledge of mapping rules and secrete key of the function. Additionally the proposed scheme is capable of not just scrambling data but it also changes the intensity of the pixels which contributes to the safety of the encryption. Steganography generally exploit human perception because human senses are not trained to look for file that has hidden information inside them. Payload is the amount of information that can be hidden in the cover object. The most widely known image steganography algorithm known as LSB technique is based on modifying the least significant bit of pixel value [2,4,8,9]. They are based on two techniques i.e. LSB replacement and LSB matching viz. Proposed steganography model is based on SDES function comprising of diffusion ,s-box mapping and secrete key. It contains Encoding function and Image retrieval.

Lili yu , Zhijuan wang and Weifeng wang [5] showed a combined encryption algorithm which is successfully made by using the simple encryption algorithm, Micro Genard encryption algorithm and the reknowned Base64 encryption algorithm.

That is, in accordance with the order of the initial encryption algorithm, the improved Micro Genard encryption algorithm and the famous Base64 encryption algorithm, the user's information is gradually encrypted, and the algorithm security is greatly enhanced. Besides, to video surveillance software system for instance, which is widely used in the field of the traffic security management, the combined encryption algorithm is completely validated, and its security is very high. The first class of transformation: if the plaintext is composed of letters, in the A-M range, the cipher text is equal to the plaintext ASCII code value plus 45 ; in the N-Z range, the cipher text is equal to the plaintext ASCII code value plus 19; in the a-m range, the cipher text is equal to the plaintext ASCII code value minus 19; in the n-z range, the cipher text is equal to the plaintext ASCII code value minus 45.The second class of transformation: if the plaintext is Arabic numbers, in the 0-4 range, the cipher text is equal to plaintext multiplied by 2 plus 1; in the 5-9 range, the cipher text is equal to plaintext multiplied by 2 minus 10. The third class of transformation: if the plaintext is other special characters, the cipher text is the same as the plaintext. Since a byte is composed of eight bits Base64 encryption algorithm try to convert 3 bytes into 4 bytes composed of 6 bits per each. According to the decimal value of each byte, using Base64 encryption algorithm to specify the character set of characters to be replaced.

Vigenere encryption algorithm uses the defined square matrix and the custom key to encrypt the plaintext message. The normal Vigenere square matrix based on twenty six capital letters, followed by cycle changing the order, composed 26 × 26 square matrix. In this paper, in order to improve the complexity of this algorithm, while improving the performance of confidentiality the following process is shown, on the basis of twenty-six Capital letters, insert ten Arabic numbers into the sequence of letters of the alphabet, with turn loop arranged in a certain order, and ultimately construct the improved. Vigenere square of 36×36 plaintext character set and key in addition to square matrix is also needed by Vigenere encryption algorithm. Initial encryption algorithm also defines Hybrid encryption algorithm.

Sankar Das, Joyshree Nath, shalabh Agarwal and Asoke Nath[6] proposed account enlightens procedure to hide a secret message in encrypted form in some non standard cover files with extensions s such as .exe, .com, .pdf, .doc, .xls, .mdb, .ppt files. Keeping in mind that, size of

secret message always must be small in comparison to cover file. Message is encrypted using MSA algorithm (2) and then they hide the encrypted message inside the non standard cover file. To hide encrypted secret message they insert the 8 bits in 2 consecutive bytes of cover file in LSB, LSB+1, LSB+2 and LSB+3 positions. This method could be very effective to hide some information in some executable file While hiding secret message in cover file we embed 1 byte information in two consecutive bytes of the cover file can hide information in almost all files except pure text or ASCII file. In Random key Matrix of size(16x16) we have to enter any text_key. Text_key size must be less than or equal to 16 characters which can be any of the 256 characters(ASCII code 0 to 255) to calculate the randomization number, the encryption number and the relative shift of characters in the starting key matrix. Relative position and the character itself are very important in method.

Monika Agarwal [7] uses three approaches of text steganography. The first approach uses the theme of missing letter puzzle and hides each character of secret message in a word by missing one or two letters in that word depending on the ASCII value of the embedded character. The second approach works by hiding message in a list of words where starting letter of word and word length is determined by the ASCII value of the character to be hidden. In the third approach, the cover comprising of paragraphs can be drawn from any source like newspaper/book. The approach conceals secret bits using start and end letter of words of cover file. Unlike the first two proposed approaches in which cover comprising of collection of words is dynamically generated, the third approach makes use of pre-existing any meaningful piece of English text as a cover file to hide the secret bits. The message is scrambled by the proposed encipher algorithm using a one-time secret key. The resulting cipher text is then hidden in cover file by an embedding algorithm using a stego key. Text steganography can be broadly classified into three types: Format based Random and Statistical generation, Linguistic methods.

Encipher function, which enciphers a message using one-time pad scheme, Hide function, which conceals the scrambled message using a stego key, Seek function, which extracts the hidden information from the stego file using the stego key, and, Decipher function, which deciphers the extracted message using the secret key are the building blocks of The model .

Mohit Garg [8] proposed a new method of hiding a secret message using text file. This process is basically called as text steganography, but the steganographic technique is slightly different because it uses html file to hide the secret message in this method the secret message is encrypted using play-fair cipher encryption mechanism which convert the message into binary format. The basic idea of this technique is that, the html documents are the fundamental elements of the web. Since the html documents are very commonly use on the internet and hence are less estimated to generate the doubt in intruder's mind for the existence of the secret message, more over any html document has considerable number of text and attributes, thus the capacity of the hiding process to hide the secret message is also high.

Akhil Kaushik, Manoj Barnela and Anant Kumar [9] focus to achieve different goals of security i.e., Availability, Confidentiality and Integrity using Block Encryption Standard for Transfer of data (BEST). This new algorithm is based on the symmetric key encryption approach. Cryptography is broadly classified into two categories depending upon the Key; which is defined as the rules used to convert a plain text into cipher text: - Private Key Encryption and Public Key Encryption. Private Key Encryption uses the same key for encryption and decryption processes. This technique is simple yet powerful but key distribution is the chief problem that needs to be addressed, two mathematically associated keys: Public Key & Private Key for encryption. The public key is available to everyone but the data once encrypted by public key of any user can only be decrypted by private key of that particular user. The process is a bit lengthy and complicated but it enhances the security aspects. Taxonomy of cryptography is the amount of plaintext that is encrypted in a single pass. The first category is known as Stream Cipher, which takes character by character of plaintext and encodes it. This process is tedious and may generate different cipher texts every time same plaintext is encrypted. Other category is Block Cipher, which reads a block of characters of plaintext and encodes it simultaneously [6]. Although, it is faster but the concern here is that same cipher text is produced every time key is applied on same plaintext[4][5]. In this paper, they have proposed a new block cipher: Block Encryption Standard for Transfer of data (BEST) Algorithm which is more secure than traditional block ciphers because it fabricates different cipher texts for same plaintext provided. The proposed algorithm has been designed in an efficient approach but avoids the sacrificing the security issues. It has been successfully implemented on the text data. We have also tried to benchmark the performance of BEST against some well-known Symmetric Key Algorithms like DES, AES and X-MODDES algorithm. This algorithm has cost-effective Block Encryption Standard technique for Transfer of data is which comparatively faster and it offers the boosted security features than the other symmetric key algorithms. Hence this algorithm proves to be a very efficient in delivering messages from sender to the receiver, achieving confidentiality as well as message authentication.

Paul.A.J,Varghese Paul, P.Mythili [10] shows a method of encryption standards such as DES (Data Encryption Standard),AES (Advanced Encryption Standard) and EES (Escrowed Encryption Standard) which are widely used to solve the problem of communication over an insecure channel. With advanced technologies in computer hardware and software, these standards seem not to be as secure and fast as one would like. In open networked systems, information is being received and misused by adversaries by means of facilitating attacks at various levels in the communication [1]. The Encryption algorithm, presented, is a simple, direct mapping

algorithm using matrix and arrays. Consequently, it is very fast and suitable for high speed encryption applications. The matrix based substitution resulting in poly alphabetic cipher text generation followed by multiple round arrays based transposing and X-OR logic based translations give strength to this encryption algorithm. Exhaustive key search is also proved inefficient for Decryption of cipher text messages created using this encryption is practically impossible. As other algorithms using 128 bits secret key but cipher text generated by this algorithm does not have one to one correspondence in terms of position of the characters in plaintext and cipher text. Brute force attacks also didn't seem to be working, which makes decryption extremely difficult.

V.Saravanan and A.Neeraja. [11] Shows today everyone use computer networks to share resource and to exchange information. This computer network can be classified into many types based on the properties like protocol, topology and architecture. Widely known topologies are bus, ring, star, mesh and hybrid. In bus topology all the nodes will connected using a single cable (this cable will act as a backbone). Damaging the cable will cause network failure. The information can be easily hacked by hackers by taping the cable anywhere in the network. The nodes in a peer-to-peer network will communicate with one another. The information exchanged by these nodes can be easily hacked by using any one or more of the hacking tools such as IP Sniffer (Build around packet sniffer), The information like bank account details, user name, password, personal details and more will be hacked by the hackers and they can misuse the same. This problem can be solved normally by using encryption and decryption algorithms (Cryptography). The process of converting readable secret information into unreadable form (Cipher Text) is called as Encryption while Decryption is a process of converting the unreadable cipher text into readable form (plain text). In proposed method, the image can be divided into number of pieces called macro blocks. Each pixel in the macro block will compare with its neighbour pixel. By doing this easily identifies whether the macro block contain plain image or not. In plain regions, only one LSB can be altered to store the data, otherwise DD will increase. It proposed a new region selection rule for steganalysis. This method makes the data embedding process to alter more LSBs of a pixel based on region type to increase the capacity of the stenography. Hence the security, capacity and DD will get improve. Face detection algorithms can be added to proposed method to increase the capacity of the stenography process.

III. Performance Analysis

Design an algorithm is not precious till it doesn't analysis properly. Proposed technique have to check whether it is a good solution or not for confidentiality.

Encryption/Decryption Analysis

To analysis encryption/decryption algorithm, some parameters have taken on which performance of algorithm is tested

To ensure whether it is strong against various attack it internal structure is tested by calculating avalanche effect and also key analysis is done for the same.

i. Time Efficiency Analysis

If an algorithm is not time efficient it doesn't matter how strong it is, it is worthless. Proposed algorithm must be time and energy efficient. So, that we can say that it is a greener algorithm and consume less energy as compared to the existing one.

There are many encryption/decryption algorithms, but still there is always a competition to develop an algorithm which will provide high security in minimum time. Time and robustness of internal structure both are the important parameters for any cryptographic algorithm. If an algorithm has robust internal structure but not a time efficient then there is no significance to use it. Such algorithms cannot be used for real time transmission or in ad-hoc networks because of the time taken by an algorithm and also if algorithm is time efficient but not secure than again it is useless.

ii.Throughput

As time efficiency is an important parameter used to measure the performance of cryptographic algorithm but, throughput is another parameter depended on time. It can be defined as the amount of text encrypted per unit time. The algorithm having higher throughput is considered better than the other.

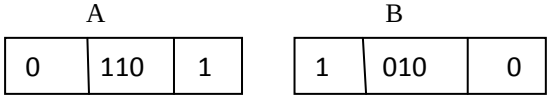
IV. Proposed Algorithm

There are many steganography algorithms, but there is a need of improvement in every algorithm. It is always required to design an algorithm which should be highly time efficient. If an algorithm is not a time efficient then it cannot be used for real time communication. Algorithm should be strong so that no one can break it. The problem in the existing system is that an algorithm which provides time efficiency is not very robust. For complete confidentiality only encryption/ decryption algorithm is not enough, it just shuffle the text in such a manner that no one understands its true meaning but there can be a chance to crack this algorithm. To provide full confidentiality encryption should be combined with steganography algorithm which hide the presence of secret transmission so that no one can guess its presence. Many different media file is used to hide these secret data, but using text file is the cheapest and efficient way.

Proposed Encryption Algorithm

Proposed encryption algorithm contains two blocks first, Encryption process and other is stegnography:

1. To perform encryption get file to be send
2. Convert the file into binary format and in a Bfile.
3. Extract the word with different end and start value.
4. Same value at start and end of the word extract in some other place.
5. Send the middle part of the word by hiding it in HTML file using some tag.

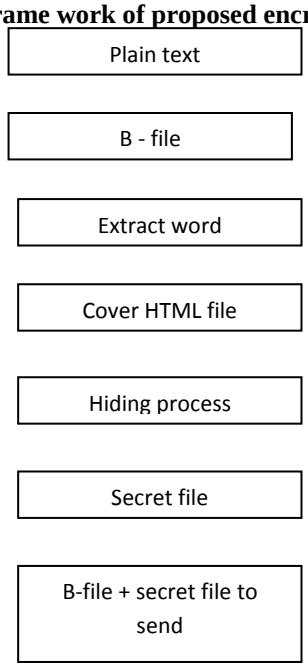


Suppose we want to send a part first then to represent 110 in HTML codes we are using here p tag. As p tag should be placed in Body tag but we are putting that tag in Head which shows the presence of some data in coding.
Syntax of <p align="left|right|center|justify">
Attribute Values

Value	Description
left	Left-align text
right	Right-align text
center	Center-align text
justify	Stretches the lines so that each line has equal width (like in newspapers and magazines)

Above tags are used to represent 110
There should not be any other <p> tag in <body> tag

Frame work of proposed encryption algorithm



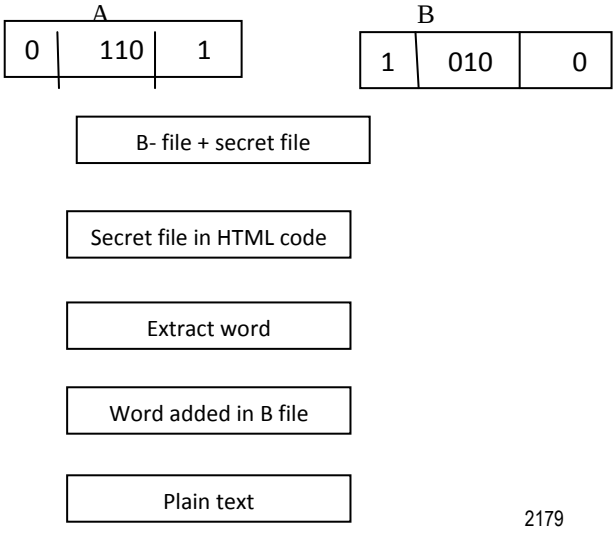
Proposed coding in HTML :-

```
<HTML>
<HEAD><TITLE>WEBPAGE</TITLE>
<style>
h1 {
   color:red;
   font-family:verdana;
   font-size:200%;

}
p  {
   color:blue;
   font-family:calibri;
   font-size:130%;
}
</style>
<style>
table, th, td {
   border: 2px solid black;
}
</style>
<p style="text-align: 'left'; font: '18pt'; courier; color: 'green'"'>
color of the sky and lake is changed.
</p>
<p style="text-align: 'left'; font: '18pt'; courier; color: 'green'"'>
color of the sky and lake is changed.
</p>
<p style="text-align: 'right'; font: '18pt'; courier; color: 'green'"'>
color of the sky and lake is changed.
</p>
</HEAD>
<BODY>
<a href="http://www.w3schools.com">This is a link</a>
<table style="width:75%">
  <tr>
    <td>Jack</td>
    <td>mith</td>
    <td>40</td>
  </tr>
  <tr>
    <td>John</td>
    <td>Jack</td>
    <td>74</td>
  </tr>
  <tr>
    <td>Ohm</td>
    <td>Don</td>
    <td>60</td>
  </tr>
</table>
</BODY>
</HTML>
```

Proposed Decryption Algorithm

Proposed decryption algorithm contains two blocks first, Encryption process and other is stegnography:

1. From received HTML coding extract the <p> tag which represent actual data and placed in head tag
2. Here left align of tag <p> in <head> tag represent presence of 1
   Here right align tag of <p> in <head> tag represents presence of 0
3. Extract actual value and merge it with the Bfile value to get actual data.
4. Convert the binary file into plain text to get the real data.



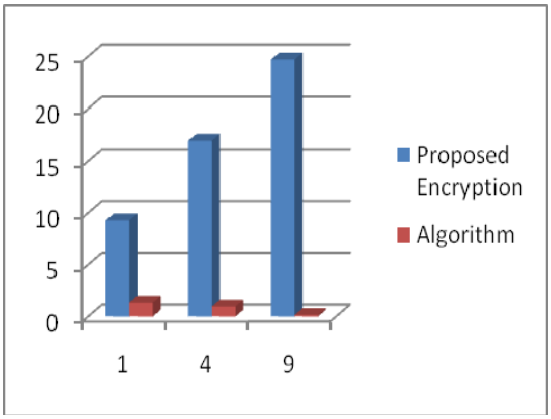
Proposed coding in HTML :-

```
<HTML>
<HEAD><TITLE>WEBPAGE</TITLE>
<style>
h1 {
   color:red;
   font-family:verdana;
   font-size:200%;

}
p  {
   color:blue;
   font-family:calibri;
   font-size:130%;
}
</style>
<style>
table, th, td {
   border: 2px solid black;
}
</style>

<p style="text-align: 'left'; font: '18pt'; courier; color:
'green'">
color of the sky and lake is changed.
</p>
<p style="text-align: 'left'; font: '18pt'; courier; color:
'green'">
color of the sky and lake is changed.
</p>
<p style="text-align: 'right'; font: '18pt'; courier; color:
'green'">
color of the sky and lake is changed.
</p>
</HEAD>
<BODY>
<a href="http://www.w3schools.com">This is a link</a>
<table style="width:75%">
  <tr>
    <td>Jack</td>
    <td>mith</td>
    <td>40</td>
  </tr>
  <tr>
    <td>John</td>
    <td>Jack</td>
    <td>74</td>
  </tr>
  <tr>
    <td>Ohm</td>
    <td>Don</td>
    <td>60</td>
  </tr>
</table>
</BODY>
</HTML>
```

PERFORMANCE ANALYSIS

File Size in KB	Algorithm	
	Proposed Encryption	Algorithm
1	9.28	1.32
4	16.99	0.96
9	24.7	0.136

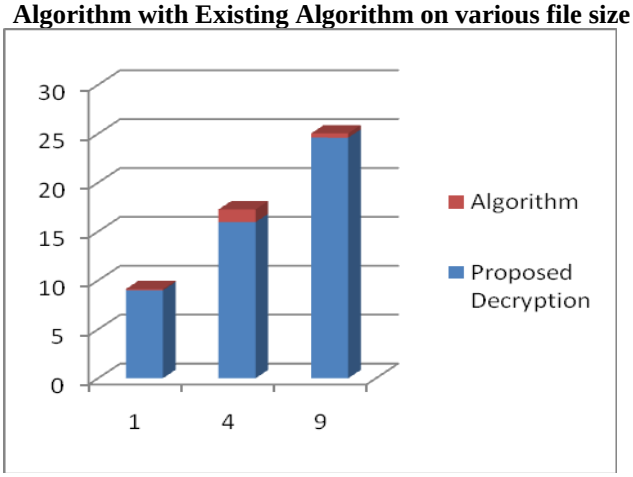
Table 1: Comparison of Proposed Encryption Algorithm with Existing Encryption Algorithm on various file size



Graph for above data (Table 1)

File Size in KB	Algorithm	
	Proposed Decryption	Algorithm
1	8.99	0.13
4	15.96	1.30
9	24.6	0.436

Table 2: Comparison of Proposed Decryption Algorithm with Existing Algorithm on various file size

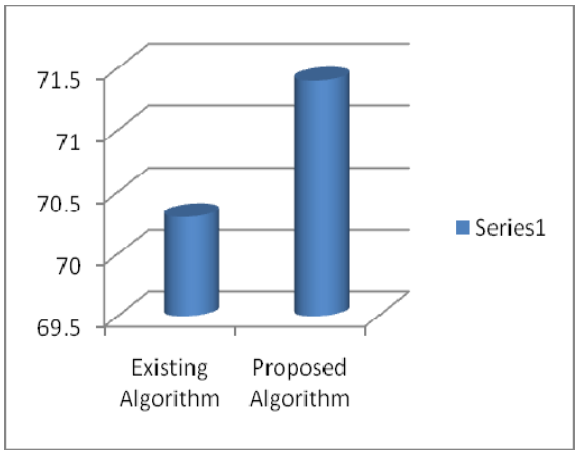


Graph for above data (Table 2)

PSNR value is used to calculate the distortion in the original image and the stego image. It is obvious that if something is hided inside, than it get distorted but this distortion should be minimum for designing the best solution. PSNR value is calculated for proposed work and compares it with the existing PSNR value.
Table 3 shows the result after calculating PSNR value.

File Size in KB	PSNR Value	
	Existing Algorithm	Proposed Algorithm
1	70.3	71.4

Table 3 PSNR comparison between Existing Algorithm and Proposed Algorithm



Graph for above data (Table 3)

V. Application Of Proposed Algorithm

Security-Proposed algorithm introduces an algorithm to hide the text data behind HTML file.Advantage of proposed technique is that it combines both cryptanalysis as well the steaganographic techiniques and hence we can declare it as more secure than any other algorithm.

Time Efficiency- Proposed algorithm is not time efficient, on the basis of results we can say that.

Robustness-Structure of encryption/decryption is very robust. Hence it support secure transmission and also used for fast transmission.

Bulk Size- In transmission it uses HTML file, size of which file is not bulky to transfer.

VI. Future Enhancement

Future enhancements which we observed in the proposed algorithm that we can improve its avalanche affect up to certain extent so that we can reach up to optimum degree of security. Another enrichment which we can introduce in this algorithm is that, its total encryption time to encrypt desired amount of secret message can also be reduce. If both these factors enhanced optimum levels then we can say that the algorithm will reach up to extra ordinary standards of performance and safety.

VII. Conclusion

As the technology changes very rapidly, demand for the security of secret data and information also changes rapidly. In this paper author proposed a new algorithm which is used to provide security on the transmitted data. Authors have design and developed a new confidentiality algorithm which is a combination of two algorithm first encryption/decryption algorithm and other is steganography algorithm. Designed algorithm is time efficient, robust, low cover file size. It is the better key that can be use for real time transmission, and transactions over network and any channel which required security.

Key feature using here is a HTML file as a cover file in steganography algorithm which makes this algorithm available for fast communication. Implementation results shows that the proposed encryption/decryption is best solution, if someone wants high security in minimum time. Also its combination with steganography gives its more potency and the proposed steganography hides the data with minimum cover file size.

References

[1] Rishav Ray, Jeeyan Sanyal, Debanjan Das, Asoke Nath. “A new Challenge of hiding any encrypted secret message inside any Text/ASCII file or in MS word file: RJDA Algorithm”. 2012 IEEE International Conference on Communication Systems and Network Technologies

[2] Clair, Bryan. “Steganography: How to Send a Secret Message.” 8 Nov. 2001.

[3] Westfeld, A., and G. Wolf, Steganography in a Video conferencing system, in proceedings of the second international workshop on information hiding, vol. 1525 of lecture notes in computer science, Springer, 1998.pp. 32-47.

[4] Johnson, N. F. and Jajodia, S, “Exploring steganography: Seeing the unseen”, IEEE Computer Magazine, pp. 26-34, February 1998.

[5] William Stallings, Cryptography and Network Security, Principles and Practice, Third edition, Pearson Education, Singapore, 2003.

[6] Symmetric Key Cryptography using Random Key generator: Asoke Nath, Saima Ghosh, Meheboob Alam Mallik: “Proceedings of International conference on security and management(SAM’10” held at Las Vegas, USA Jul 12-15, 2010), P-Vol-2, 239-244(2010).

[7] An Integrated Symmetric key Cryptography Algorithm using Generalised modified Vernam Cipher method and DJSA method: DJMNA symmetric key algorithm : Debanjan Das, Joyshree Nath, Megholova Mukherjee, Neha Choudhary, Asoke Nath: Communicated for publication in IEEE International conference WICT 2011 to be held at Mumbai Dec 11-14, 2011.

[8] Data Hiding and Retrieval: Asoke Nath, Sankar Das, Amlan Chakraborty, published in IEEE “Proceedings of International Conference on Computational Intelligence and Communication Networks (CICN 2010)” held from 26-28 NOV’ 2010 at Bhopal.

[9] Advanced Steganographic approach for hiding encrypted secret message in LSB, LSB+1, LSB+2, LSB+3 bits in non standard cover files : Joyshree Nath, Sankar Das, Shalabh Agarwal and Asoke Nath, International Journal of Computer Applications, Vol- 14, No. 7, Page-31-35, Feb (2011).

[10] Advanced Steganography Algorithm using encrypted secret message: Joyshree Nath and Asoke Nath, International Journal of Computer Science and Applications, Vol-2, No. 3, Page- 19-24, Mar (2010).

[11] A Challenge in hiding encrypted message in LSB and LSB+1 bit positions in any cover files: executable files, Microsoft Office files and database files, image files, audio and video files : Joyshree Nath, Sankar Das, Shalabh Agarwal and Asoke Nath : JGRCS, Vol-2, No. 4, Page- 180-185, Apr (2011).

[12] New Data Hiding Algorithm in MATLAB using Encrypted secret message: Agniswar Dutta, Abhirup Kumar Sen, Sankar Das, Shalabh Agarwal and Asoke Nath : Proceedings of IEEE CSNT- 2011 held at SMVDU (Jammu), 03-06 Jun, 2011, Page 262-267.

[13] New Steganography algorithm using encrypted secret message: Joyshree Nath, Meheboob Alam Mallik, Saima Ghosh and Asoke Nath : Proceedings of Worldcomp 2011 held at Las Vegas (USA), 18-21 Jul, 2011.

[14] Steganography In Digital Media: Principles, Algorithms and Applications by Jessica Fridrich : Cambridge University Press.

[15] Cryptography and Network Security, William Stallings, Prentice Hall of India.

[16] Cryptography & Network Security, Behrouz A. Forouzan, Tata McGraw Hill Book Company.

[17] Cryptography and Information Security, V. K. Pachghare, Prentice Hall of India.

[18] Data Security and Privacy Protection Issues in Cloud Computing, Deyan Chen, Hong Zhao
[19] Efficient Security Solution for Privacy-Preserving Cloud Services Lukas Malina and Jan Hajny
[20] Xing Tang, Mingsong Chen," Design And Implementation Of Information Hiding System Based On RGB", Consumer Electronics, Communications and Networks (CECNet), IEEE-2013
[21] Rishav Ray, Jeeyan Sanyal, Debanjan Das, Asoke Nath, A new Challenge of hiding any encrypted secret message inside any Text/ASCII file or in MS word file: RJDA Algorithm", 2012 International Conference on Communication Systems and Network Technologies,IEEE-2012