ISSN:0975-9646

A Nobel Approach of Providing Confidentiality over Text Data with High PSNR Value

Harsh Deepak Shrivastava[1], Sushil Tiwari[2], Sriram Yadav[3]

[1]*M.Tech. Scholar, Department of Computer Science & Engineering, MIT, Bhopal (M.P.), INDIA*
[2] *Assoc.Professor, Department of Computer Science & Engineering, MIT, Bhopal (M.P.), INDIA*
[3] *Asst.Professor & Head, Department of Computer Science & Engineering, MIT, Bhopal (M.P.), INDIA*

***Abstract* - With the rapid development in the era of internet and networking technologies, there is always a requirement to improve the security system which secures the transmitted data over unsecure channel. Many cryptographic algorithms have been designed to ensure the security. Encryption/Decryption algorithms and Steganography algorithms are used to provide confidentiality. There is always a competition to design and develop an algorithm which not only secure but also be time efficient. In this paper, Authors have proposed a new model which is not only secure but also time efficient too. This paper proposed a new way of steganography which hided the data behind the text file with a reduced cover size than the existing.**

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

I. INTRODUCTION

Today, almost each and every person is dependent on internet. Everyone shares their personal, professional or public information over internet. There is always a requirement to keep the professional and public information secret. It is a big issue in today's world. With the rapid development in modern technologies and internet, designing and development of new algorithms are always required. To keep data secure many cryptography and steganography algorithms have been designed but with the time, updating of these algorithms is must. In today's scenario security is not only concern but also time efficiency required with high security. Existing algorithms fails to provide these needs. If an algorithm is highly secure than also it takes high time to ensure that integrity and if the algorithm is time efficient than it is less secure. Also adapting of new techniques with new features are also required.

Encryption/Decryption Algorithm are used to keep data confidential. It shuffles the data in such a way that no one other than authenticated person can read the data. Ensuring of authenticated person is determined by key used to encrypt and decrypt the data. Encryption / Decryption algorithm can be categorized in two ways on the basis of type of key. First, Symmetric Key Algorithm and second Asymmetric Key Algorithm. In Symmetric Key algorithm both sender and receiver uses the same key to encrypt or decrypt the data. While Asymmetric Key algorithm uses two different key at both ends, one key is used for encryption called public key and the other key is used for decryption called private key. Also the encryption/decryption algorithm can be categorized the way, how data is processed. One stream cipher and other is block cipher. In stream cipher, processing is done on each bit or character and in block cipher first the data is divided into equal size block and then processing is done on each block.

Steganography on the other hand is another technique to provide confidentiality. Here secret data hide behind any other cover file such that no one can detect the presence of secret data. This method is very much similar to the concept of invisible ink used earlier. Again, there are many algorithms proposed for steganography but there is always a competition to develop an algorithm which is more efficient than other. Efficiency can be calculated by calculating PSNR value and cover file size. According to today's scenario it is required to develop an algorithm which should have low cover file size as well as high PSNR value. PSNR value is used to calculate the distortion in cover file.

II PROPOSED WORK

In order to fulfill the requirement authors have design and developed a new algorithm to ensure the confidentiality. Idea for designing this algorithm was to develop an algorithm which should enough strong so that it can use for unsecure channel and also should be time efficient so that it can used for real time communication. The proposed structure is a combination of two algorithms encryption/decryption algorithm and steganography algorithm. The combination of

both the algorithm is striking feature of this proposed work. Also to keep the algorithm light, word file is used as a cover file rather than image file. Here, data hide behind every characters using color component of each character. Proposed algorithm is inspired with the algorithm proposed in paper [1]. This paper also proposed its own architecture which is a combination of both encryption/decryption algorithm and steganography algorithm. But after implementing this paper authors have found that there is a chance of improvement in terms of time efficiency in encryption algorithm and cover file size in steganography algorithm. Proposed work focus on these points and design an algorithm parallel to it which have all the properties similar but also having low cover file size and high time efficiency than paper [1].

A. Proposed Encryption / Decryption Algorithm

To overcome the problem discussed earlier, authors have proposed a new symmetric key cryptographic algorithm. This algorithm is divided into two part, first key generation and second encryption block which convert plaintext to cipher text. The block diagram of proposed encryption algorithm is shown in Figure 1 and Figure 2.

Proposed Encryption Algorithm

Proposed encryption algorithm is divided into two parts; its first part is key generation and second is encryption, Key Generation technique generates X keys which is used to encrypt the message. Steps for key generation techniques are as follow:

1. First, user entered 16 character key is converted into 128 bit.
2. These 128 bits are used to generate a random number X. This random number is dependent on user entered key. ASCII values of all the characters are added and then modulus of 32 on the summation result is calculated. The result is random number represented by X.
3. Now, the user entered 128 bits are divided into two 64 bits block.
4. These 64 bits are interchanged with each other and then left 64 bits XORed with right 64 bits and the result is used as new right 64 bits. Also the left 64 bits shifted 9 bits left.
5. Now, both the block again divided into 32 bits block and get shuffled as shown in Figure 1.
6. Concatenation Block concatenates all the four 32 bits block and produces a 128 bit stream.
7. Now, H box perform xor operation on each bits with its X position bit.
8. These process is repeated X times and generates X random keys (Key_1, Key_2, ….., Key_x)

Now, Steps used in encryption technique are as follows:

1. The complete message is converted into bit stream.
2. Now, the whole plaintext is divided into number of block such that each block has 128 bits. If the last block have less bits than padding of zero is done.
3. Now, the process will takes X rounds and at each round different keys will be used.
4. In each round plaintext bits are xored wit key_i and then go to the H-Box. The functionality of H-Box is same as discussed in key generation.
5. The result of first round is passing as an input for the next round.

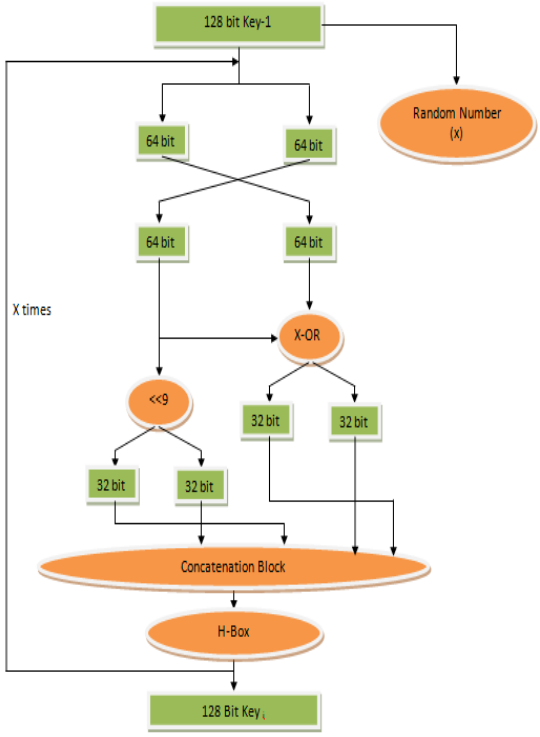

Figure1. Key Generation of proposed Encryption/Decryption Algorithm.

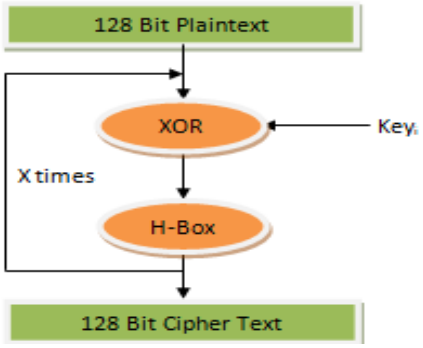

Figure 2. Proposed Encryption Block.

Proposed Decryption Algorithm

Proposed decryption algorithm is reverse process of proposed encryption algorithm.

1. Key Generation: Key generation of decryption algorithm is same as in encryption algorithm.
2. Decryption Block: Decryption of proposed algorithm is shown in Figure 3. Steps of decryption block are as follows:
   a. First cipher text is divided into numbers of blocks where each block contains 128 bits.
   b. For each block, repeat the following steps
      i) 128 bits cipher text is passed to the reverse H-Box, which is reverse process of H-Box
      ii) and then it XOR to the ker in reverse order.
   c. If all the blocks are completed then exit.

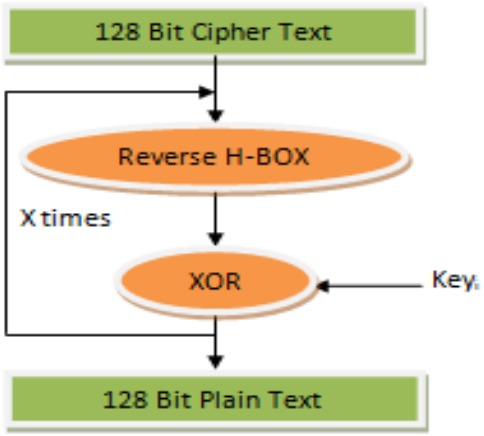

Figure 3. Proposed Decryption Block.

B. Proposed Steganography Algorithm

Proposed Encryption/Decryption algorithm is enough strong to ensure the confidentiality, but to increase the security, such that unauthorized person even cannot guess the presence of some secret transmission the proposed algorithm combined with proposed steganography algorithm. To make this combination of two algorithm efficient authors used a MS-Word file as a cover file. Steps of proposed steganography algorithm are as follow:

1. Calculate the length of secret text and represent it with 32 binary numbers.
2. Convert the whole secret text into binary format and append the length before the binary secret message.
3. Hide three bits of secret at least significant bit of each color component of characters.
4. Repeat step three till all the bits hide behind the character.

III. Performance Analysis

In this section, authors have discussed the performance of proposed work against the paper [1]. For better comparisons authors have calculated the performance of each algorithms separately, Firstly authors have compared the encryption algorithm against encryption algorithm used in paper[1] and then compare its steganography algorithm again with steganography algorithm discussed in paper[1].

A. Encryption/Decryption Analysis

To check the strength and efficiency of proposed encryption algorithm, Avalanche Effect, Timing and Key Analysis is done.

Robustness of Proposed Encryption Algorithm:

Robustness of proposed encryption/ decryption algorithm can be calculated by avalanche effect. According to avalanche effect, changing a single bit in key will change fifty percent cipher text. The algorithm closed to avalanche effect considered more robust than the algorithm far from avalanche effect. Table 1 shows the avalanche effect comparison of proposed algorithm with paper [1]. It is clearly seen from Table 1 that Avalanche effect of proposed work is better than avalanche effect of paper 1.

TABLE 1
AVALANCHE COMPARISON BETWEEN RJDA AND PROPOSED ALGORITHM

File Size in KB	Avalanche Effect	
	RJDA Algorithm	Proposed Algorithm
Single bit change in key	42.1875	48.94%

Graphical Representation of avalanche effect comparison is shown in Figure 4.

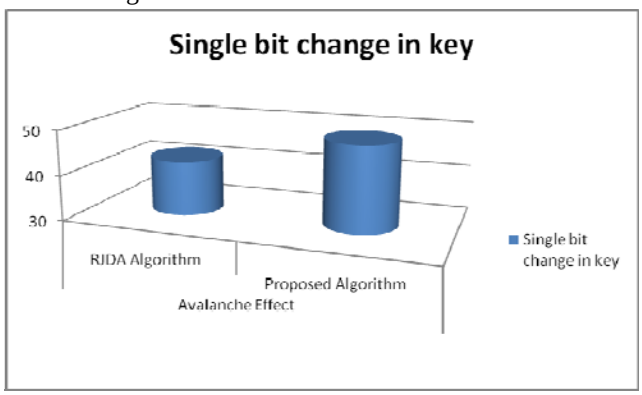

Figure 4. Avalanche comparison between RJDA and Proposed Algorithm

Timing Analysis of Proposed Algorithm

To design a better solution, strength cannot be the only parameter, Timing of processing also keep importance. An algorithm which gives high strength in less time is more

valuable than other. In this section authors have discussed the timing analysis of proposed algorithm with the paper [1].

TABLE 2
COMPARISON OF PROPOSED ENCRYPTION ALGORITHM WITH PAPER [1] ENCRYPTION ALGORITHM ON VARIOUS FILE SIZE

File Size in KB	**Algorithm**	
	Execution Time in Second	
	Paper [1]	Proposed Encryption Algorithm
1 KB	8.658	0.150
5 KB	16.582	0.915
10 KB	24.663	2.145

TABLE 3
COMPARISON OF PROPOSED DECRYPTION ALGORITHM WITH PAPER [1] DECRYPTION ALGORITHM ON VARIOUS FILE SIZE

File Size in KB	**Algorithm**	
	Execution Time in Second	
	Paper [1]	Proposed Decryption Algorithm
1 KB	8.672	0.148
5 KB	16.358	0.886
10 KB	24.363	2.042

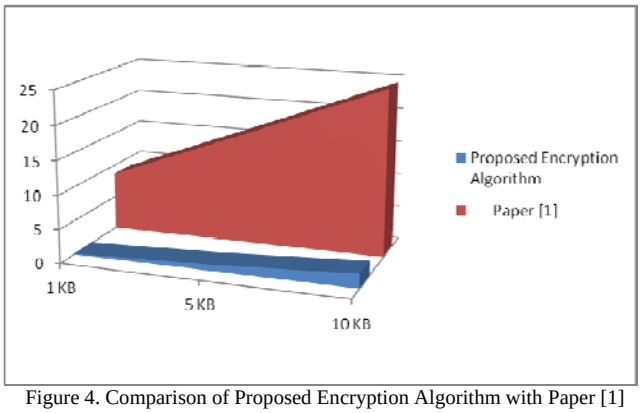

Figure 4. Comparison of Proposed Encryption Algorithm with Paper [1] Encryption Algorithm on various file size

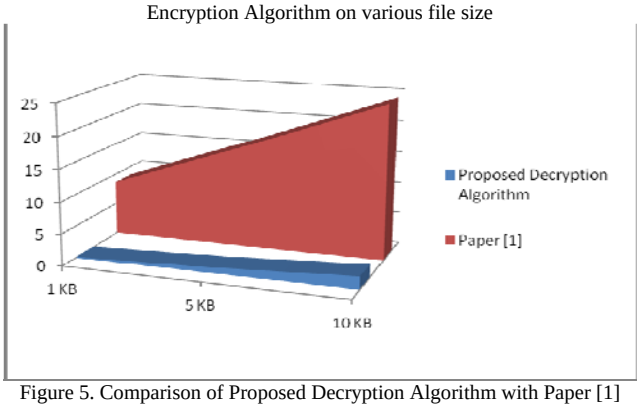

Figure 5. Comparison of Proposed Decryption Algorithm with Paper [1] Decryption Algorithm on various file size

Implementation result shown in Table 2 and Table 3, clearly proved that Proposed encryption/ decryption algorithm is far better solution than the solution presented by paper [1]. Proposed Encryption/ Decryption algorithm is time efficient. Graphical representation of Table 2 and Table 3 is shown in Figure 4 and Figure 5.

Key Analysis

Proposed encryption algorithm uses 128 bit key, which is enough strong against any attack. Security of any algorithm is dependent on key, if some intruder get succeed to gain access over secret key, then the whole security in algorithm is completely waste. Brute force attack required 2^n combination to break a key of length n bits. From this, proposed algorithm requires 2^{128} combination to break the key.

B. Proposed Steganography Algorithm

In this section, authors have analysis on steganography algorithm. The key feature of the proposed steganography algorithm is that it uses text as cover file rather than using image as a cover file. The problem behind image is that it uses high bandwidth during transmission which makes the algorithm slow. The analysis of proposed steganography algorithm is done on the basis of PSNR value and Cover file size.

PSNR value

PSNR value is used to calculate the distortion in the cover file during hiding process. A steganography algorithm is considered a better algorithm if its distortion is minimum. It is found that PSNR value of proposed work is high which proves it strength.

Cover File Size:

Cover file size is another parameter used to calculate the efficiency of steganography algorithm. If the size of cover file is less as compared to other than it requires less bandwidth and hence transmission time is less but for a large cover file more bandwidth is required and required more time for transmission. Here, every three bits of secret message are hide behind every character, whereas in paper [1] bits are hide behind the spaces. Hiding behind spaces makes the cover file size large as compared to hiding behind every character.

III. CONCLUSION

With the changes in technologies in this modern world, there was a requirement to develop and design an algorithm which provides high security in less time. This paper focuses on confidentiality. Authors have developed a confidentiality algorithm which is a combination of proposed cryptographic encryption/decryption algorithm and proposed steganography algorithm. The key feature here is using world file as a cover

file in steganography algorithm which makes this algorithm available for fast communication. Authors have shown with their implementation results that the proposed encryption/decryption is best solution, if someone wants high security in minimum time. Also its combination with steganography gives its more strength. Again 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 International Conference on Communication Systems and Network Technologies,IEEE-2012

[2] Manoj Kumar Ramaiya, Naveen Hemrajani, Anil Kishore Saxena, "Security Improvisation in Image Steganography using DES", IEEE-2012.

[3] Thomas Leontin Philjon. J, Venkateshvara Rao. N, Metamorphic Cryptography -A Paradox between Cryptography and Steganography Using Dynamic Encryption, IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011.

[4] Yambin Jina Chanu , Themrichon Tuithung , Kh Manglem singh," A Short Survey on Image Steganography and Steganalysis Technique " , IEEE Trans, 2012 science and Management (ICAESM- 2012) 709 -713.

[5] W. Luo, F. Huang, J. Huang, Edge adaptive image steganography based on LSB matching revisited, IEEE Trans. Inf. Forens. Security 5 (2) (2010) 201-214.

[6] Ge Huayong, Huang Mingsheng, Wang Qian , "Steganography and Steganalysis Based on Digital Image", IEEE Trans. International Congress on Image and Signal Processing,(2011) 252-255.

[7] Amitava Nag, Saswati Ghosh, Sushanta Biswas, Debasree Sarkar, Parta Pratim Sarkar " An Image Steganography Technique using X-Box Mapping", IEEE Trans. International Conference Advances in Engineering,

[8] Guilliang Zhu, Weiping Wang, "Digital Image Encryption algorithm based on pixel", ICIS – 2010 IEEE International Conference 29-31 Oct 2010, pp – 769 – 772.

[9] Jasmin Cosic , Miroslav Bacai, " Steganography and Steganalysis Does Local web Site contain "Stego" Contain " , 52 th IEEE Trans. International Symposium ELMAR-2010, Zadar, Croatia 2009 ,pp 85 –88.

[10] Zhang Yun-peng , Liu Wei " Digital Image Encryption Algorithm Based on chaos and improved DES ", System, man and Cybernatics ,SMC 2009 , IEEE International Conference 11-14 Oct 2009, pp 474-479.

[11] Saeed R. Khosravirad, Taraneh Eghlidos and Sharokh Ghaemmaghami, "Higher Order Statistical of Random LSB Steganography", IEEE Trans. 2009, pp 629 - 632.

[12] J. Mielikainen, LSB Matching Revisited, IEEE Signal Process. Lett. 13 (5) (2006) 285-287.

[13] N Provos and P. Honeyman, "Hide and seek: An Introduction to Steganography", IEEE Security and Privacy, 2003, pp32-44.

[14] Donovan Artz" Digital Steganography: Hiding Data within Data ", Los Alamos National Laboratory, IEEE Trans. 2001, pp 75-80.

[15] K Suresh Babu , K B Raja, Kiran Kumar k, Manjula Devi T H, Venugopal K R, L M Pathnaik" Authentication of Secrete Information in Image Steganography", IEEE Trans. 13.

[16] Moerland, T, "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, www.liacs.nl/home/ trnoerl/privtech.pdf.

[17] Schaefer " A Simplified Data Encryption Standard Algorithm", Cryptologia, January 1996

[18] Data Encryption Standard : http://csrc.nist.gov/publications/fips /fips 46-3 /fips- 46-3.pdf

[19] Advanced Encryption Standard http://csrc.nist.gov/publications/ fips/fips197/fips- 197.pdf

[20] Cryptography and network Security Principles and Practices, Charles Fleeger

[21] William Stallings, "Network Security Essentials (Applications and Standards)", Pearson Education, 2004.