A Novel Approach of Designing Cryptographic Algorithm with High Confidentiality

Shubhi Jain
M.Tech. Scholar, Department of Computer Science & Engineering, NRI, Bhopal (M.P.), INDIA

Sini Shibu
Professor, Department of Computer Science & Engineering, NRI, Bhopal (M.P.), INDIA

ABSTRACT
Today's in modern world security is the main issue while communication. Internet is main source for communication but also it is not as much secure as it assume. For secure transmission of data many algorithms have been developed. Steganography and encryption/decryption algorithms are used for confidentiality. Some times to improve the security both the algorithms are combined. There is always a trade to develop an algorithm which provides high security in less time than the existing one. This paper proposed a new structure called HCCA (High Confidentiality Cryptography Algorithm) which is a combination of encryption/decryption and steganography algorithm. The key feature of this algorithm is that it is highly secure, time efficient and required small cover file.

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

1. INTRODUCTION
With the rapid development in computer technology, security of secret data is main concern. Many researches have been done on this. When someone talks about security, it is talking about authentication, integrity and confidentiality. This paper is focusing on confidentiality. Confidentiality means storing or transmitting secret data from one end to another such that only authenticated person can access the actual information or data. If unauthorized person try to gain this data it should be a waste for him. Two types of algorithms are used to provide confidentiality, first Encryption/ Decryption algorithm and second steganography algorithm.

Encryption/Decryption algorithm is an algorithm which shuffles the data in such a way that no one can understand the actual meaning of data. This shuffling is done on the basis of key, only the person who have the key will reshuffle and get the actual data. Encryption/Decryption algorithm can be categorized on the basis of key: Symmetric key algorithm and Asymmetric key algorithm. In Symmetric key algorithm, encryption and decryption both the algorithm share the same key. In asymmetric key algorithm pair of key is generated, one key is used to encrypt and another is used to decrypt.

There are many Encryption/ Decryption algorithms that are developed to provide confidentiality but to check best algorithm some parameters are used to measure them such as timing to check its time efficiency, Avalanche effect to check the strength of algorithm, key size to check its security against various attack, memory requirement etc.

On the other hand, steganography algorithm is used to hide the secret information behind multimedia file like text file, image file, audio file or video file. In encryption/decryption algorithm, unauthorized person can get access to the data but they can't understand the true meaning of data, it is garbage for them but here unauthorized person or intruders cannot guess the presence of secret data.

Again there are many steganography algorithms, but there are some parameters which is used to find the best algorithm i.e. cover file size and PSNR (peak signal to noise ratio) to calculate the distortion. If the algorithm uses less size of cover file and havin high PSNR value consider better algorithm than other.

In this paper, authors have proposed two new algorithms; one is encryption/decryption and second is steganography algorithm and combine them and called it HCCA (High Confidentiality Cryptography Algorithm). Authors have presented their implementation results and compare it with latest research on this domain and find that their proposed algorithm HCCA is highly secure, time efficient, uses less cover file in size and high PSNR value.

2. PROPOSED WORK
The proposed work is a combination of symmetric key encryption/decryption algorithm which shuffles the data in such a way that no intruder can understand the true meaning of secret data and second steganography algorithm which then hide the ciphertext (output of encryption algorithm) behind the image file.

2.1 Proposed HCCA Encryption / Decryption Algorithm
It is a block cipher symmetric key algorithm which shares the same copy of key at both the end (sender end and receiver end). It uses a key of size 128 bits which is used to generate two more keys which are used for encryption and decryption process. Also this algorithm divides the plaintext or secret data into blocks of 128 bits and then performs encryption or decryption process on it. Proposed HCCA encryption/decryption takes three rounds and all the three rounds use different keys.

2.1.1 Proposed HCCA Encryption Algorithm
Steps of proposed HCCA encryption algorithm are as follows:

1. Key Generation: HCCA algorithm uses three keys, the process of generating three keys are as follows:
    a. Take 128 bits from user.
    b. Perform XOR operation of entire key bits from its right bit and the resultant output is key2. This operation is named Modified XOR in Figure 2.
    c. Repeat step 2 once more to generate key3, taking key 2 as an input.

2. **Encryption Block:** Encryption block of a proposed HCCA encryption is shown in Figure 2. Steps to encrypt a secret data are as follows:

   d. First complete secret data is divided into a block of 128 bits. If the last block is contain less bits than pad 0 bits till it becomes equal to 128.

   e. Take first 128 bit block and perform XOR operation with key1.

   f. Repeat the step b for key2 and key 3.

   g. The outcome of step c is cipher text of first 128 bit.

   h. Repeat step a to step d for all the 128 bit plaintext.

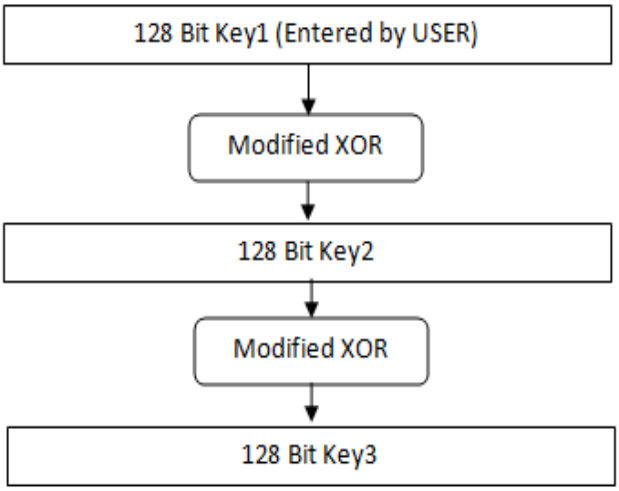

Figure1. Key Generation of proposed HCCA Encryption/Decryption Algorithm.

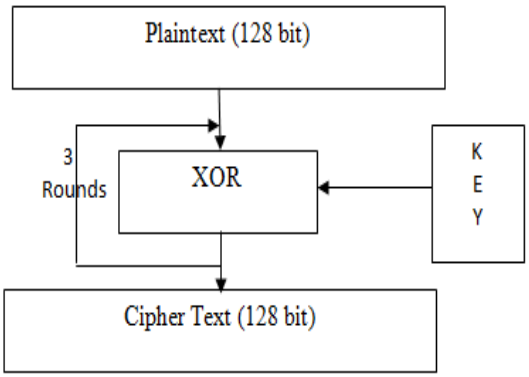

Figure 2. Proposed HCCA Encryption Block.

2.1.2 Proposed HCCA Decryption Algorithm

Proposed HCCA decryption algorithm is reverse of proposed HCCA encryption algorithm. Steps of decrypting the cipher text are as follows:

1. Key Generation: Key generation of decryption algorithm is same as in encryption algorithm.
2. Decryption Block: Decryption of proposed HCCA 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) XOR the cipher text with key 3 then the result is further xor with key 2 and then with key 1.

      ii) The outcome of step i is Plaintext of first 128 bits cipher text.

   c. If all the blocks are completed then exit.

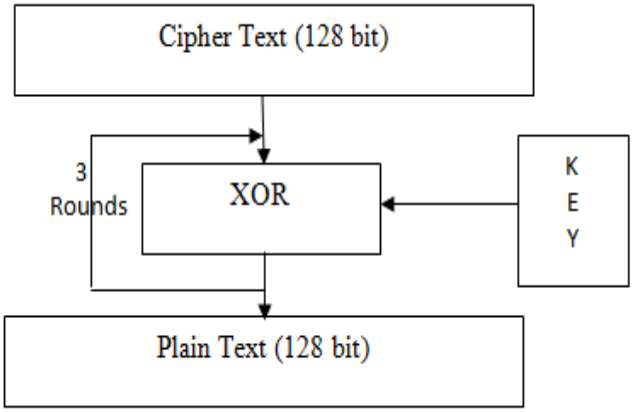

Figure 3. Proposed HCCA Decryption Block.

2.1.3 Proposed HCCA Steganography Algorithm

There are many steganography algorithms, but there is always a competition to develop an algorithm which uses small cover file in size and also having high PSNR value. But both the parameter are inversely proportional to each other. Keeping all these in mind, here authors have proposed a new technique which improves the PSNR value without increasing cover file size. Here cover file size is constant. Proposed HCCA Steganography Algorithm uses traditional LSB method but with some modification. This modification improves the PSNR value. This algorithm uses image as cover file with a limitation that the size of image should be eight by three times of number of characters in cipher text. It hides each bit of cipher text behind each component (R, G, B) of each pixel using LSB method.

Proposed HCCA Steganography algorithm is divided into three steps.

1. *Traditional LSB Method:* In this step, Ciphertext is hide behind the image cover file using LSB method. This method hide entire bits of cipher text behind each red, green and blue component of each pixel using LSB method.

   for example if cipher text is 1011 and four pixels value are 10101010, 11001100, 11100010, 11000111 then after applying LSB method 1011 is hide behind four pixels like

   10101011, 11001010, 11100011, 11000111

2. *Analysis:* In this step, Analysis of entire pixel is done. four sets have been prepared 00, 01, 10 and 11. Now, all pixels whose sixth and seventh bits are 00 will comes under 00 set, similarly those pixels whose sixth and seventh bits are 01, or 10 or 11 will comes under set 01 or 10 or 11 respectively.

   Now changes in each set have been analyze like out of total pixels of that set how many pixels have changed.

   For example: In previous example set having bits 01 at sixth and seventh position out of three pixels two pixels have changed and pixel is unchanged.

3. *Decision:* In this step decision has taken, if the changed pixels are more than unchanged pixels than invert all the pixel of that set otherwise keep them as it is.

   For example: In previous example out of three, two pixels are changed after inverting the pixels will be 10101010, 11001011, 11100010, and 11000111**.** It means only one pixels is changed out of three. Repeat these steps for all the sets.

3. PERFORMANCE ANALYSIS

This section gives the performance analysis of proposed algorithm and compares it with existing algorithms. Authors have proposed two algorithms and also compare them separately. There are many different parameters which are used to analyze an algorithm. Authors uses three parameters Timing analysis, Avalanche effect and key analysis to show the strength of proposed HCCA encryption algorithm and PSNR value to show the strength of steganography algorithm.

3.1 Encryption/Decryption Analysis

To show the strength of proposed HCCA encryption algorithm timing analysis, avalanche effect and key analysis has been done and compare it with research paper [1] and [2].

3.1.1 Timing Analysis

The main parameter to analyze any algorithm is its speed. It is important for any algorithm to be time efficient especially when it also used for real time situation. Table 1 shows the comparison of timing with different size of files.

Figure 4 and Figure 5 shows the graphical representation of Table 1 and Table 2. It is clearly seen from the graphical representation that proposed algorithm is highly time efficient. The experimental result is tasted on fifty sample files and average of them is presented here. Now because proposed algorithm is time efficient hence it can be used for real time communication so that data can be transmitted secretly without much delay.

3.1.2 Avalanche Effect

Avalanche effect is another parameter to analyze the strength of algorithm. According to avalanche effect a change of single bit in a key will change 50% changes on cipher text but this is ideal condition, an algorithm closed to avalanche effect is considered more secure. Table 3 shows experimental results after calculating avalanche effect of proposed and existing algorithm.

Table 1: Comparison of Encryption Time of Proposed Algorithm on Various File Size in seconds

File Size in KB	**Algorithm**		
	Execution Time in Second		
	Proposed HCCA Algorithm	Steganography using DES[1]	Dynamic Encryption [2]
1 KB	0.018	0.027	0.075
6 KB	0.908	1.575	2.172

3.1.3 Key Analysis

Proposed algorithm uses 128 bits key and generate two more keys which are used to encrypt and decrypt of secret data. According to brute force attack combination required to break the key it needs 2128 combination. It is near to impossible to calculate this value even from supercomputer. Hence it can be say that it is highly secure against brute force attack.

Table 2: Comparison of Decryption Time of Proposed HCCA Algorithm on Various File Size

File Size in KB	**Algorithm**		
	Execution Time in Second		
	Proposed HCCA Algorithm	Steganography using DES[1]	Dynamic Encryption [2]
1 KB	0.011	0.031	0.087
6 KB	0.889	1.582	2.175

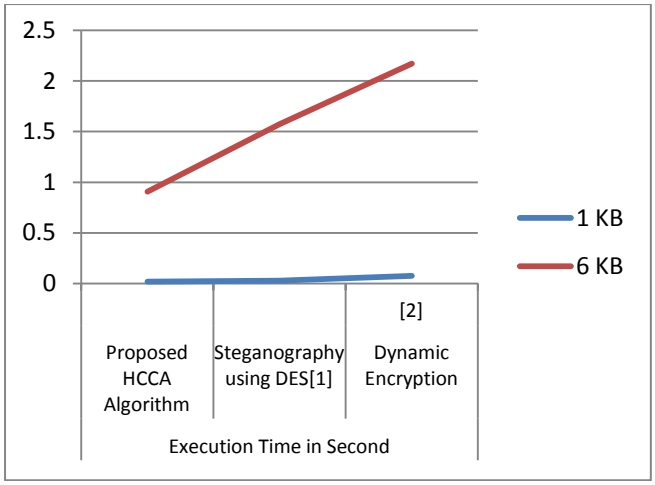

Figure 3: Encryption time of the proposed HCCA algorithm

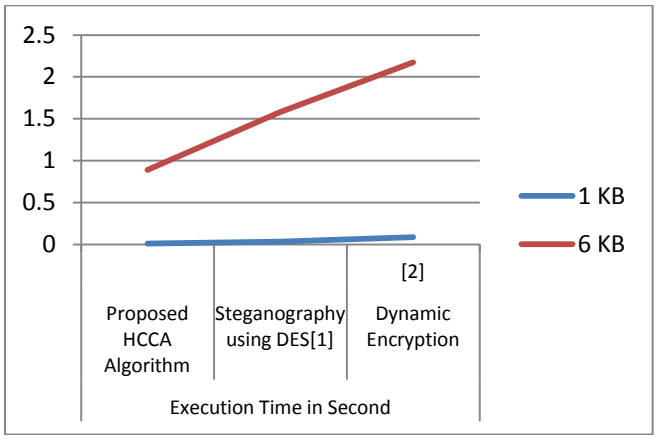

Figure 4: Decryption time of the proposed HCCA algorithm

Table 3 Avalanche Effect of Proposed HCCA Algorithm

File Size in KB	Proposed HCCA Algorithm	Steganography using DES[1]	Dynamic Encryption [2]
Key-1 (ABCD)	49.63%	49.41%	48.01%
Key-2 (ABCE)			

3.2 Proposed HCCA Steganography Algorithm

To analyze the proposed HCCA steganography algorithm PSNR value and cover file size is analyzed.

3.2.1 PSNR value

PSNR is the peak signal to noise ratio. It is used to calculate the deviation of stego image with the original image. If the PSNR value of an algorithm is high, it means deviation of stego image with respect to original image is less. If the deviation of the stego-image with the original image is less it means it means it is hard to detect the presence of secret hiding but if deviation is more it mean easy to detect the presence of secret hiding.

Authors have compared the PSNR values of proposed algorithm Table 4.

Graphical representation of Table 4 is shown in Figure 5. It is clearly seen from here that proposed HCCA algorithm have high PSNR value than other existing algorithms.

Table 3: Comparison of PSNR values between Paper [1] and Paper [2]

	Algorithm		
PSNR Value	Proposed HCCA Algorithm	Steganography using DES[1]	Dynamic Encryption [2]
	55.63	52.644	37.71

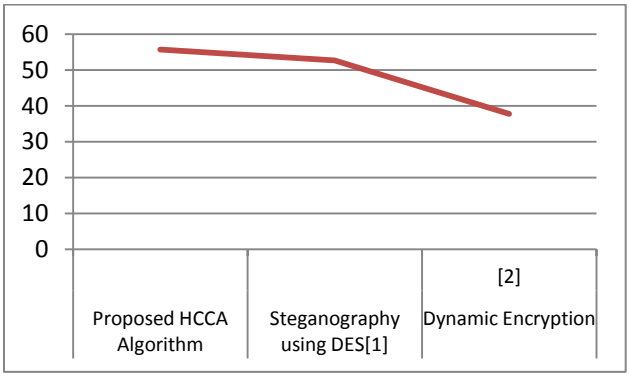

Figure 5: Comparison of PSNR values between Proposed HCCA, Paper[1] and Paper[2]

Cover File Size: It is a parameter that is used to calculate the efficiency of steganography algorithm. It is necessary to keep the size of cover file should be less. If the cover file size is large than the transmission time will also increases. Here, each pixel contains three bits. Each component (R, G, B) of each pixel hide one bit. Hence the cover file size required to hide the secret data should eight/three of the original size of secret data.

4. CONCLUSION

This paper presents new algorithms to provide high security over transmitted data. Authors have combined its two proposed algorithm in such a way that after combining both, a user will get high confidentiality, authentication and integrity. Implementation results show that proposed HCCA encryption algorithm and steganography algorithm is time efficient, highly secure and having less distortion. HCCA can be used for real time communication and also it is suitable for AD-HOC network because of its time efficiency, it consumes less battery.

5. REFERENCES

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

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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,

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

[8] 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.

[9] 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.

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

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

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

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

[14] 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.

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

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

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

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

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

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