Research Journal of Applied Sciences, Engineering and Technology 4(6): 608-614, 2012
ISSN: 2040-7467

Submitted: September 29, 2011 Accepted: November 04, 2011 Published: March 15, 2012

A Hybrid Approach for Security Enhancement by Compressed Crypto-Stegno Scheme

[1]G. Manikandan, [1]N. Sairam and [3]M. Kamarasan
[1]School of Computing, SASTRA University, Thanjavur-613401, Tamil Nadu, India
[3]Senior Programmer, CSE Department, Annamalai University,
Chidambaram-608002, Tamil Nadu, India

Abstract: In this study we propose a new hybrid technique of combining "the twins" cryptography, Steganography along with the compression techniques which results in a new extreme of providing informational security. The importance of information not only depends upon its contents but also upon its safety arrival to the receiver. Nowadays, eavesdropping one's personal messages and exposing it to the air becomes passion of showing one's technical expertise to the world. There are numerous occurrences of breaching of message contents even where the data equipped with the techniques of Steganography and cryptography. So, a need for "practically unbreakable and non suspicious systems" becomes vital. Our experimental results shows that our system is unique in its design and as well as in its performance when compared to a specific steganographic or a cryptographic technique.

Key words: Blowfish, cryptography, f-function, lossless compression, security, steganography

INTRODUCTION

Steganography and Cryptography are well known and widely used techniques that manipulate information in order to hide or crypt their existence. More specifically, Steganography is the art and science of communicating in a way which hides the existence of the communication. Thus a Steganographic system hides the content inside any multimedia content and this process of hiding the text inside a image or an audio file or a video file is referred as "Embedding process". On the other hand, cryptography protects information by transforming it into an unreadable format (Stallings, 1999). The original text is transformed into a scramble equivalent text called cipher text and this process is called as "Encryption". This is achieved via an Encryption Algorithm. Only those who possess a secret key can decrypt the cipher text into plaintext. Steganography and Cryptography are cousins in the spy craft family: the former hides the message so it cannot be seen; the latter scrambles a message so it cannot be understood.

There are a number of ways to enhance the security of different cryptographic and steganographic schemes. One of the best ways to strengthen a cryptographic scheme is to increase the strength of its key. Manikandan *et al.* (2011) suggest a method to improve the strength of the key in case of RC4 algorithm.

Sairam *et al*. (2011) proposed an approach to improve the security by using multilevel cryptographic schemes.

Another interesting approach is to combine the two basic forms of ciphers, namely block cipher and stream cipher (Manikandan *et al*., 2011). This approach was studied further and instead of using both the type of ciphers on the plain text (Manikandan *et al*., 2011) suggested a method in which one was used with the plain text and the other with the key.

Vaithiyanathan *et al*. (2010), proposed an approach to decrease the execution time of blowfish algorithm by using a modified F-function.

This study is an extension to (Manikandan *et al*., 2011) where cryptography and steganography was integrated in order to improve the security. In the approach presented in this paper, the combination of steganography and cryptography is further strengthened by including a compression technique before using the encryption process.

LITERATURE REVIEW

Cryptography: Cryptography is the study and practice of protecting information by data encoding and transformation techniques (Stallings, 1999). There are two types of cryptographic schemes available on the basis of key:

- **Symmetric key cryptography:** This is the cryptographic scheme which uses a common key for enciphering and deciphering the message.
- **Asymmetric or public key cryptography:** This type of cryptographic scheme uses two keys for encryption and decryption called Public key and Private Keys.

Corresponding Author: G. Manikandan, Assistant Professor, School of Computing, SASTRA University, Thanjavur-613401, Tamil Nadu, India

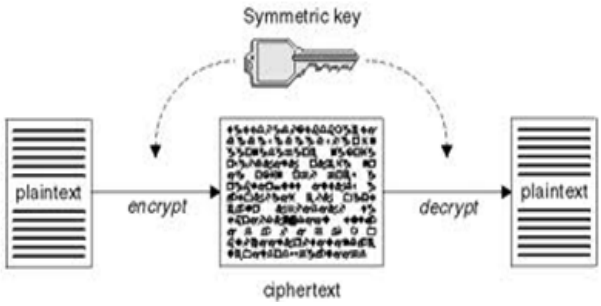

Fig. 1: Symmetric key cryptography

We adopted Symmetric key cryptographic scheme as shown in Fig. 1. In this only one key is needed for communication. So, the chosen cryptographic scheme involves:

- Plaintext: The original message that has to be communicated to receiver.
- **Encryption:** Enciphering of data by using a key via a desired encryption algorithm at sender side.
- **Transmission:** Transfer of cipher message to receiver through a public communication channel.
- **Decryption:** Deciphering of the cipher text thus received via the same algorithm (reverse Encryption) by using the key.

•We can also classify symmetric key cryptography into two types on the basis of their operations as:

- **Stream ciphers:** It is a symmetric key cipher where plaintext bits are combined with a pseudorandom cipher bit stream (key stream), typically by an exclusive-or (XOR) operation. In a stream cipher the plaintext digits are encrypted one at a time
- **Block ciphers:** It is also a symmetric key cipher operating on fixed-length groups of bits, called blocks. A block cipher encryption algorithm takes an n-bit block of plaintext as input, and produces a corresponding n-bit output block of cipher text.

We have chosen block cipher for our cryptographic operation since it is the main tool for implementing private key encryption in practice.

Steganography: This is a type of security technique which is of the form "security through obscurity". Steganography is the art of hiding and transmitting data through apparently innocuous carriers in an effort to conceal the existence of data.(Domenico and Luca, 2007). In this method the data which is to be sent is concealed in any multimedia file like image, video or an audio file. There are many famous steganographic techniques exist worldwide. The most frequently used techniques are:

- LSB Insertion
- Fingerprinting and Watermarking
- Transform Based Steganography
- Public key Steganography

We have taken LSB Insertion method in which the data is hidden inside the Least Significant Bits of the image. On the basis of hiding the text inside the multimedia contents, we can classify the Steganography into:

- Image steganography
- Audio steganography
- Video steganography

We are going to deal with Image Steganography and hence hereafter if we refer Steganography it actually refers to image Steganography. This approach consists of following terminologies:

- **Plaintext:** The original data that has to be communicated to the recipient.
- **Cover image:** An Image which is acts as a cover in which the secret message is to be concealed.
- **Embedding process:** The process of embedding or inserting the secret text into the cover image with the help of any Steganographic algorithm.
- **Steg image:** The image resulted after the completion of embedding process which looks as exactly as the cover image without any suspicion of the presence of secret text inside it.
- **Extraction process:** The process of extracting or revealing the original message from a received Steg image by using the same Steganographic algorithm that the sender has chosen.

Compression: Compression is a technique which is used to compress or encode a plaintext in to a compressed text which not only removes redundant data but also improves storage utilization. An another significant feature of compression is improves Bandwidth which fastens the

communication .In General, Compression can be classified into:

- **Lossy compression:** A Non-reversible compression technique which may leads to loss or fidelity of data.
- **Lossless compression:** A reversible technique will not affect or alter the data.

We use lossless Compression Techniques for our hybrid model since it does not affect or alter the original data.

Lossless compression : Lossless compression maintains a table which contains some table entries that are replaced for repeated strings of data. Hence decompression of it becomes completely feasible. Moreover Lossless compression techniques are highly context based and hence losslessness is achieved. We adopted LZW (Lempel-Ziv-Welch) algorithm because it is fast and easy to implement.

PROPOSED SYSTEM

We effectively combined Compression, Crypto and Stegno model and derived a new hybrid model. We made this attempt in order to make the system theoretically and practically unbreakable. This Hybrid approach will surely enhance the performance and security and the steps are to be taken place in the following order:

- Getting Plaintext which is to be sent to the recipient from the user.
- Plaintext is compressed by encoding it in LZW Compression algorithm which produces a new plaintext.
- Transformation of plaintext in to cipher text by undergoing an encryption process using the modified cryptographic algorithm.
- The third step will be embedding process and thus obtained cipher text is hided inside any cover image using a Steganographic algorithm.
- Thus the resulted Steg image is communicated through any communication channel to the receiver.

The inverse of these steps will be taken place in the receiver side which are as follows:

- Extraction Process will be carried out first which separates the embedded message from the Steg image.
- Thus obtained message will be in the scrambled form, so decryption process should be carried out by following the modified cryptographic Decryption process.
- Finally, the receiver can able to read the actual secret message sent at the sender's end by decompressing it.

The Fig. 2 represents our proposed CCS model in the form of a block diagram.

Compression of data: This LZW algorithmencodes 8-bit data into fixed-length 12-bit codes. As soon as the encoding starts, the first 0 to 255 represents 1-character sequences each corresponds to 8-bit character, and the remaining codes 256 to 4095 are created in a dictionary whenever the corresponding data is encountered. Whenever the code for the sequence is encountered a new code is added to the dictionary. The dictionary maintains single-character strings which corresponds to all the possible input characters. LZW scans the input string for successively longer substrings until it finds s sequence which is missing in the dictionary. As soon as it encounters with such string the substring which is longer than all substrings present in that dictionary is retrieved sent to output, and thus obtained new string is appended to the dictionary table with the next code that is available. Hence, the last input character is utilized as the succeeding starting point for the next scan. (Welch, 1984)

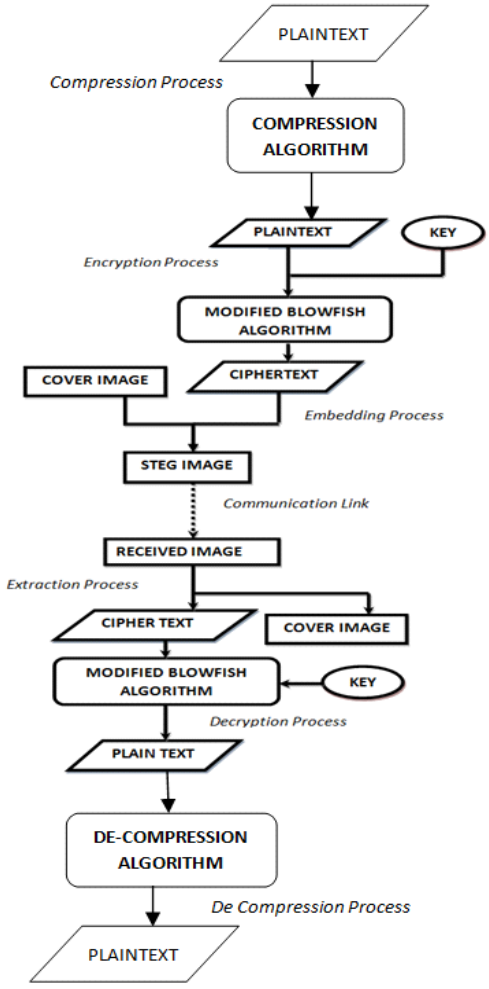

Fig. 2: CCSM (Compressed crypto-stegano model)

Cryptographic approach: In this study, the Blowfish encryption algorithm is chosen for Encryption since:

- It is fast, strong and free and hence an alternative to existing encryption algorithms (Schneier, 1994).
- It uses only simple operators which include addition, table lookup and XOR. The table includes four S-boxes (256~32bits) and a P-array (lXx32bits). Blowfish is a cipher based on 16 Feistel rounds, and the design of the F-function used amounts to a simplification of the principles used in DES to provide the same security with greater speed and efficiency in software (Schneier, 1994).

BLOWFISH ALGORITHM

Blowfish, a symmetric block cipher uses a Feistel network, 16 rounds of iterative encryption and decryption functional design. The block size of blowfish algorithm is 64 bits, and the size of the key may be of any length but having a maximum range till 448 bits. The power of the Blowfish algorithm relies on its sub-key generation and its encryption. Blowfish cipher uses 18 P-boxes and four Substitution boxes each of 32 bit size. It uses a Fiestal cipher which is a general method of transforming a function into another function by using the concept of permutation. The Fiestal Structure of blowfish algorithm is shown in the Fig. 3.

Modified F-function: Function F plays an important role in the algorithm, and we decided to modify function F. Original function F is defined as follows. (Schneier, 1995):

$$F(X) = ((S_1 + S_2 \bmod 2^{32}) \text{ XOR } S_3) + S_4 \bmod 2^{32}$$

Instead, we modified the F-Function by replacing 2 addition operations as XOR Operations and one circular shift operation. Thus the modified F-Function is written as:

$$F(X) = CS ((S1 \text{ XOR } S2 \bmod 2^{32}) + (S3 \text{ XOR } S4 \bmod 2^{32}))$$

This modification leads to the parallel execution of two XOR operations. In the case of original F-function which executes in sequential order and it requires 32 Addition operations and 16 XOR operations. But in the case of our modified F-function it requires the same 48 gate operations (32-XOR, 16-addition) but time taken to execute these 48 operations will be reduced because of parallelism. We executed 32 XOR operations in parallel order using threads and hence time taken to complete 16 gate operations will be equal to the time taken to complete 32 XOR operations since we are running it in parallel environment (Kishnamurthy *et al*., 2006). After that we are performing 32 bit circular shift operation which further enhances the security of the system. The Fig. 4 and Fig. 5 represent the existing and the modified F-function respectively.

Steganographic approach: In the case of Steganographic algorithm we chooses LSB Hiding algorithm which hides the very presence of the text inside an image. Least Significant Bit (LSB) insertion is a simple approach to hide information in any multimedia cover file: it overwrites the LSB of a pixel with an M's bit. We can able to hide 3 bits per pixel in a 24-bit cover image. Hence the resulting Steg image will make no difference to the cover image to human eyes. (Neil *et al*., 2003)

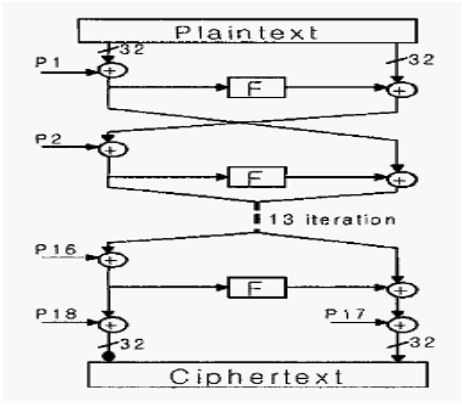

Fig. 3: Fiestal structure of blowfish algorithm

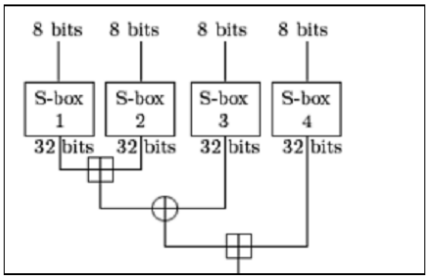

Fig. 4: Existing F-function

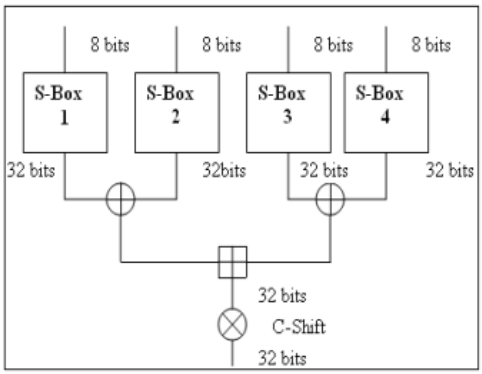

Fig. 5: Modified F-function

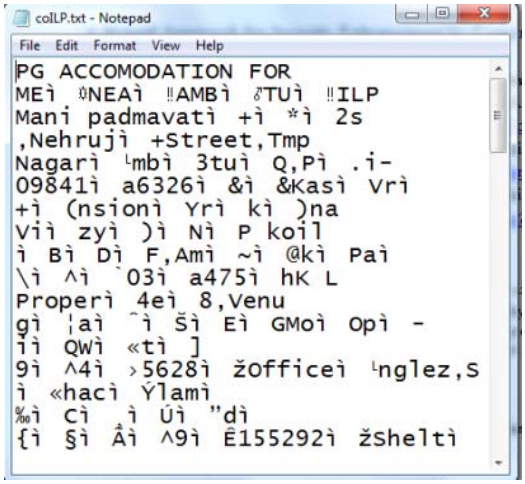

Fig. 6: Sample text after compression

Significance of the hybrid model:

- We adopted the three important techniques which determine the security of the data. They are:
  - Enciphering and Deciphering phase with the Cryptography
  - Embedding and Extraction of data with the Steganography
  - Compression and decompression of message with LZW
- It is to be noted that we can able to hide only 14% of the JPEG file dimension in a JPEG image (Kishnamurthy *et al*., 2006). So compression of plaintext favours the chance of hiding some more data in a JPEG image and makes the embedding process more feasible.
- While F-function is executed, time taken to perform 32 logical operations in sequential order is considerably reduced to time taken to perform 16 logical operations due to parallelism (Kishnamurthy *et al*., 2006).
- It's quite hard for the eavesdroppers to realize that the F-function is modified and hence probability of attack is less on comparing with the original Blowfish algorithm.
- If in case Steganalysis is performed and hence the LSB algorithm is breaked, there is yet another struggle for intruders to cryptanalysis the cipher text which is considered to be very hard as far as the strength of Blowfish algorithm is concerned.

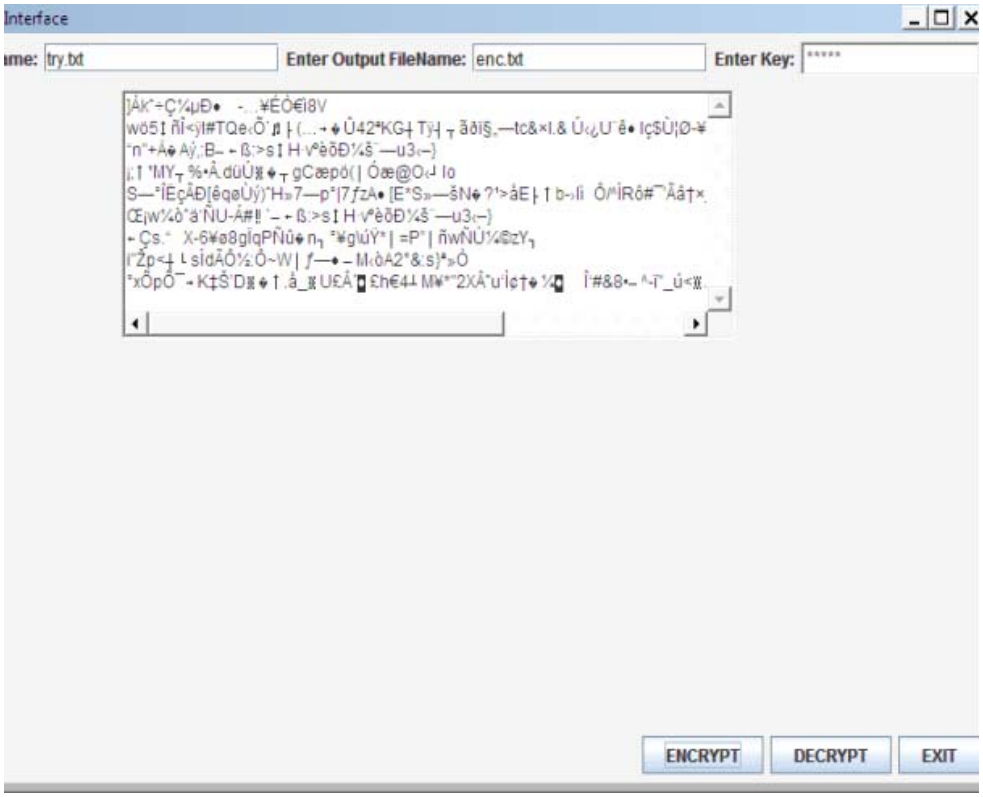

Fig. 7: Encryption process

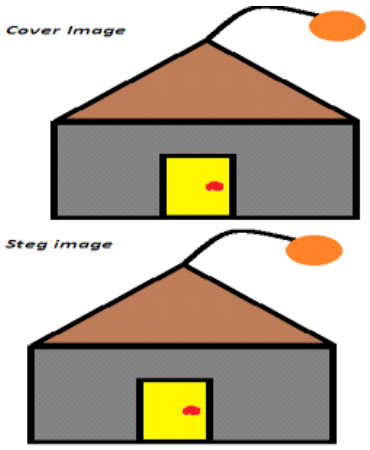

Fig. 8:Cover image and steg image

Simulation: We simulate the hybrid compressed crypto stegano model using Java Development Kit, because of its better GUI features, robustness and platform independent features. Figure 6 shows the plain text after being compressed. Figure 7 is a snapshot of the encryption process. The cover as well as the stegno image is shown in Fig. 8. In Fig. 9 the extracted compressed text is shown. Finally Fig. 10, represents the original plain text after the decompression process.

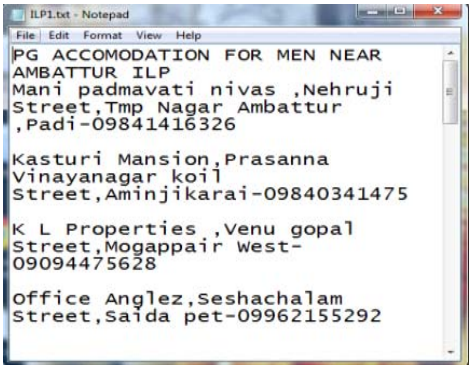

Fig. 10: Text after decompression

CONCLUSION

In this study we have presented a novel method for enhancing security by integrating Compression, Cryptography and Steganography. We have proven that this hybrid approach is both an effective steganographic method as well as a theoretically unbreakable cryptographic one since the F-function used in Blowfish algorithm is modified and hence hard to guess.

ACKNOWLEDGMENT

The Experiments are conducted in the ICT Lab, School of Computing, SASTRA University. The

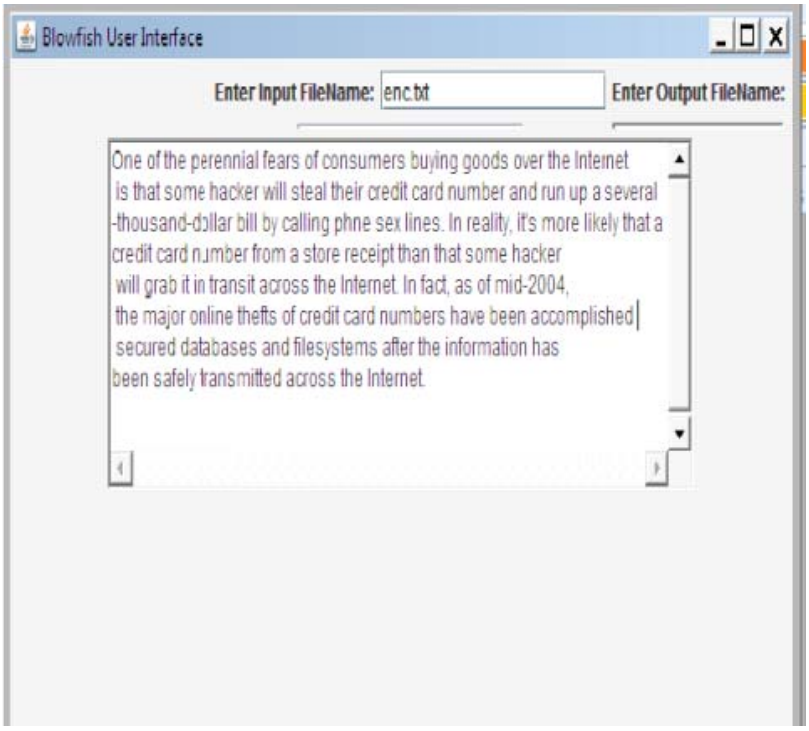

Fig. 9: Extraction process

Authors would like to thank the Associate Dean, ICT Department, SASTRA University for providing the facilities.

REFERENCE

Domenico, B. and I. Luca, 2007. Image based Steganography and cryptography. International Conference on computer vision.

Kishnamurthy, G.N., V. Ramaswamy and G.H. Leela, 2006. Performance Enhancement of Blowfish algorithm by modifying its function. Proceedings of International Conference on Computers, Information, System Sciences and Engineering, University of Bridgeport, Bridgeport, CT, USA, pp: 240-244.

Manikandan, G., R. Manikandan and G. SundarGanesh, 2011a. A new approach for generating strong key in RC4 algorithm. J. Theor. Appl. Info. Technol., 24(2): 113-119.

Manikandan, G., G.D.R. Krishnan and N. Sairam, 2011b. A unified block and stream cipher based file encryption. J. Global Res. Comp. Sci., 2(7): 53-57.

Manikandan, G., R. Manikandan, P. Rajendiran, G. Krishnan and G. SundarGanesh, 2011c. An integrated block and stream cipher approach for key enhancement. J. Theor. Appl. Info. Technol., 28(2): 83-87.

Manikandan, G., M. Kamarasan, P. Rajendiran and R. Manikandan, 2011. A Hybrid Approach for Security Enhancement by modified Crypto-Stegno scheme. Eur. J. Sci. Res., 60(2): 224-230.

Neil, F.J., D. Zoran and J. Sushil, 2003. Information Hiding: Steganography and Watermarking: Attacks and Countermeasures. 3rd Edn., Kluwer Academic Publishers.

Sairam, N., G. Manikandan and G. Krishnan, 2011. A novel approach for data security enhancement using multi level encryption scheme. Inter. J. Comp. Sci. Info. Technol., 2(1): 469-473.

Stallings, W., 1999. Cryptography and Network Security: Principles and Practices. 2nd Edn., Prentice Hall, Country.

Schneier, B., 1994. Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish). Fast Software Encryption, Cambridge Security Workshop proceedings (December 1993), Springer-Verlag, pp: 191-204.

Schneier, B., 1995. Applied Cryptography: Protocols, Algorithms and Source Code in C. 2nd Edn., John Wiley & Sons.

Vaithiyanathan, V., G. Manikandan and G. Krishnan, 2010. A novel approach to the performance and security enhancement using blowfish algorithm. Inter. J. Adv. Res. Comp. Sci., 1(4): 451-454.

Welch, T.A.,1984. A technique for high-performance data compression. Comp., 17(6): 8-19.