Result Evaluation of Twice Precaution during Transmission of hidden data using RC4 algorithm.

Amrapali Bhandare, Dinesh Patil & Rahul Shete,
Students of BE (COMPUTER),
Under the guidance of Prof.Sonawane V.D.
Al-Ameen College of engineering, Koregaon Bhima, Pune.

ABSTRACT:-"Twice precaution during transmission of hidden data" introduces the security solution for protecting information . The data owner deals with the transmission of abundant dataover the unsafe bandwidth limited communication. As a data is not safe some data. The receiver uses the data hiding key to retrieve the accommodated data even though the receiver is unaware with the original image contents. Receiver uses the encryption key so as to retrieve data so it can obtain the image which is similar to original uncompacted image. But receiver not able to retrieve the original data, for that receiver requires data hiding key also.

Keywords:- image & data encryption, image & data decryption, RC4 algorithm, image embedding etc.

(I) INTRODUCTION

To provide privacy protection, encryption converts the ordinary signal into unintelligible data. So that the traditional signal processing usually takes place before encryption or after decryption. However, in some scenarios the sender does not trust the processing service provider. So that to send a secret data without knowledge to the unauthorized person the data is encrypted and generate the encrypted key which is send to the receiver. If the receiver is the authorized person then the receiver decrypt over a network communication, the data owner encrypts the original uncompacted image by using encryption key. Then after the LSB (Least Significant Bit)of the image is compacted to create the thinly dispersed or scattered space so that it can adjust the
the data by using encryption key. The traditional way of securely and efficiently transmitting redundant data is to first compress the data to reduce the redundancy and then to encrypt the compressed data to mask its meaning. That mean the sender should encrypt the original data and network provider may tend to compress the encrypted data. At receiver side, a decoder integrating decompression and decryption function will be used to reconstruct the original data.

(II) PROPOSED SYSTEM

In the 1st phase, we do the data encryption by selecting the any random data file from the browser. Then that data file is embedding into any random image file selected from the browser. That image file is then encrypted.

In the 2nd phase, we do the image decryption by using the keys generated at the time of encryption. As soon as the image is decrypted the original data file is appear.

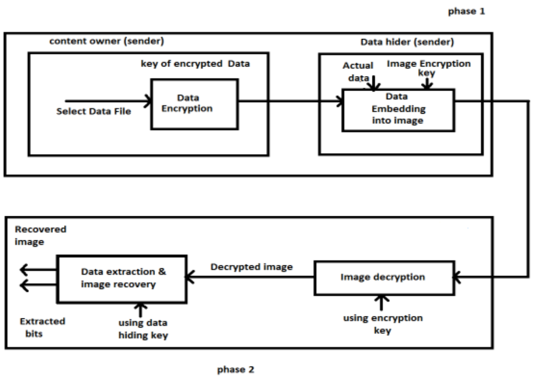

Fig:- Concept of Proposed System.

What is RC4 Algorithm?

RC4 is a stream cipher, symmetric key algorithm. The same algorithm is used for both encryption and decryption as the data stream is simply XORed with the generated key sequence. The key stream is completely independent of the plaintext used. It uses a variable length key from 1 to 256 bit to initialize a 256-bit state table. The state table is used for subsequent generation of pseudo-random bits and then to generate a pseudo-random stream which is XORed with the plaintext to give the cipher text .

1) Image Selection & Encryption Module:-

A) Image Encryption Types

Image encryption involves generation of encryption key and generation of pseudo-random sequence.

B) Generation of Encryption Key

Encryption key is 128 bit value. It is generated randomly by using the random function. The random function generates the random key in an uniformly distributed function.

C) Generation of Pseudo-Random Sequence

Pseudo random sequence consists of random bits generated using the encryption key. In our system, RC-4 algorithm is used to create the pseudo-random sequence using the 128-bitencryption key. It is represented as sequence of bytes (An array of bytes) .The number of bytes generated should be equal to the number of pixels in the input image provided the pixels are represented as 8-bit values. If the pixels are represented as 16-bit values then the number bytes in pseudorandom sequence should be double the number of pixels.

2) Data Embedding Module:-

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar. In the data embedding phase, some parameters are embedded into a small number of encrypted pixels, and the LSB of the other encrypted pixels are compressed to create a space for accommodating the additional data and the original data at the positions occupied by the parameters. According to a data-hiding key, data hider pseudo-randomly selects Np encrypted pixels that will be used to carry the parameters for data hiding.

Here, Np is a small positive integer, for example, Np=20.The other (N-Np) encrypted pixels are pseudo randomly permuted and divided into a number of groups, each of which contains L pixels. The permutation way is also determined by the data-hiding key. For each pixel-group, collect the M least significant bits of the L pixels, and denote them as B (k, 1), B (k, 2)…B (k, M. L) where k is a group index within [1, (N-Np)/L] and M is a positive integer less than 5. The data-hider also generates a matrix G sized (M.L-S)×M.L, which is composed of two parts. G= [IM.L-SQ] (1) While the left part is an (M.L-S) × (M.L-S) identity matrix, the right part Q sized (M.L-S) ×S is a pseudo-random binary matrix derived from the data-hiding key. Here, S is a small positive integer. Then, embed the values of the parameters M, L and S into the LSB of NP selected encrypted pixels. For the example of NP=20 the data-hider may represent the values of M,L and S as 2,14 and 4 bits, respectively and replace the LSB of selected encrypted pixels with the 20 bits.

3) Data-Extraction & Image-Recovery Module:-

The proposed scheme is made up of image encryption, data embedding and data-extraction image-recovery phases. The content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image. Then, the data-hider compresses the least significant bits (LSB) of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. At the receiver side, the data embedded in the created space can be easily retrieved from the encrypted image containing additional data according to the data-hiding key. Since the data embedding only affects the LSB, a decryption with the encryption key can result in an image similar to the original version [4]. When using both of the encryption and data-hiding keys, the embedded additional data can be successfully extracted and the original image can be perfectly recovered by exploiting the spatial correlation in natural image.

(III) RESULT ANALYSIS

After the test result, we get the proposed system very much advanced then existing system. Because proposed system takes less time for execution than existing system as well as the accuracy of proposed system is also more than existing system which can be clearly illustrated by following graphs & charts representation.

The following Table & Figure illustrate the actual concept of our project at which distinguish between existing system & proposed system is illustrated. It shows testing accuracy by table as well as graphical representation.

Table 1:-Testing accuracy of existing & proposed system

Sr.no.	**Module name**	**Testing Accuracy in existing system**	**Testing Accuracy in proposed system**
1	Data Encryption Module.	65%	98%
2	Data Embedding Module.	70%	95%
3	Image Encryption Module.	82%	97%
4	Image Decryption Module	85%	96%

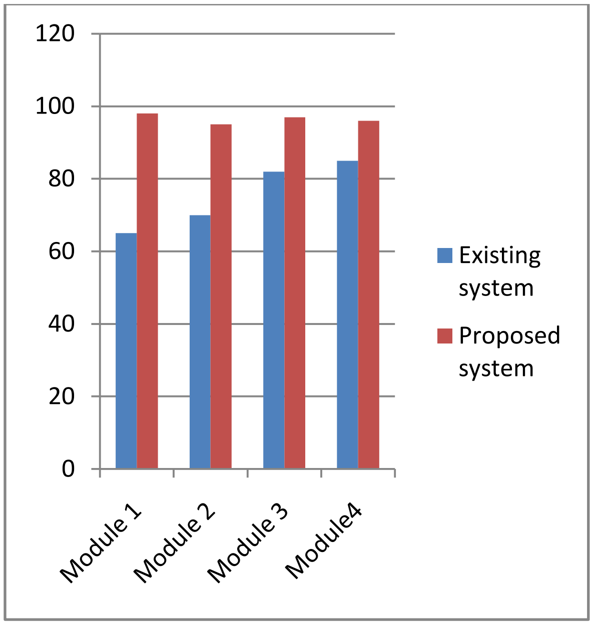

Fig 1:- Graphical representation of testing accuracy of existing & proposed system

(IV) FUTURE SCOPE

In our system,

(1) We can do some modification such as we can go for audio or video encryption & decryption in future.

(2) We can increase the size of image file which is not more than 100 kb in current proposed system.

(3) We can increase the size of data file which is also less in current proposed system.

(V) CONCLUSION

Here we have presented the way i.e. RC4 algorithm to transmission of data very securely over a network & reduces the probability of data hacking. A content owner encrypts the original uncompressed image using an encryption key. Then, a data-hider may compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate some additional data. Using data hiding key the receiver can extract additional data even the receiver has no information about the original image content

(VI) ADVANTAGES

(1) Compared with the other algorithms, the proposed system demonstrated successful accuracy in recovering the original images

(2) Less chances of hacking

(3) More reliable

(4) Reduces the time & space complexity.

(5) More secure than other algorithm of data encryption

(VII) APPLICATION

(1) It will provide data security in military sites information of any country

(2) It will provide data security in online transaction

(3) It will provide security in banking transaction

(4) It will provide data security in social side accessing

(VIII) REFERENCES

1) X. Zhang, “Lossy compression and iterative reconstruction for encrypted image,” IEEE Trans. Inform. Forensics Security, vol. 6, no. 1, pp. 53–58, Feb. 2011.

2) W. Liu, W. Zeng, L. Dong, and Q. Yao, “Efficient compression of encrypted grayscale images,” IEEE Trans. Image Process., vol. 19, no. 4, pp. 1097–1102, Apr. 2010.

3) T. Bianchi, A. Piva, and M. Barni, “Composite signal representation for fast and storage efficient processing of encrypted signals,” IEEE Trans. Inform. Forensics Security, vol. 5, no. 1, pp. 180–187, Feb. 2010.

4) S. Lian, Z. Liu, Z. Ren, and H. Wang, “Commutative encryption and watermarking in video compression,” IEEE Trans. Circuits Syst. Video Technol., vol. 17, no. 6, pp. 774–778, Jun. 2007.

5) Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, “Reversible data hiding,” IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354– 362, Mar.2006.

6) M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, “On compressing encrypted data,” IEEE Trans. Signal Process, vol. 52, no. 10, pp. 2992–3006, Oct. 2004.

7) Glover, P. and M. Grant, Digital Communications, 2nd edition, Person Education, 2004.

8) Springer, 2003. MJoset Pieprzyk, ET. al., Fundamentals of Computer Security,