www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 3 March 2015, Page No. 10868-10871

Twice Precaution during Transmission of Hidden Data

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.

smtbhandare47@gmail.com /patildinesh85@gmail.com /rahulshete2011@yahoo.com

ABSTRACT

Now days, every single human being is addicted by technology. Technology becomes one of the basic needs. So, we have also responsible for the data which is transmitting over the network. We have to maintain the records, security & oppose the hacking that data from the third persons. Therefore our group focus on these issues & try to implement such kind of system which is comprises in the class of 'data security' which named as "Twice Precaution during Transmission of hidden data".

There are two phases included in our system. 1st phase is depends upon image & data encryption. 2nd phase is depends upon recovery of that image & data. After encrypting image & data, the encrypted data is embedded into the encrypted image. At the end of 1st phase, we get image encryption key & after embedding the data into image, we get data hiding key.

Both keys, encrypted form of image & data is transmitted to receiver at another end side. Both keys are essential to decrypt image & data successfully. After decryption we get the original image as well as data.

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

INTRODUCTION

To provide privacy protection, encryption converts the ordinary signal into unintelligible data. That's why; in existing system data is visible to sender before encryption or visible to receiver 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 encrypted key is generated by doing the data encryption then the key is send to the receiver.

If the receiver is the authorized person then the receiver decrypts 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.

RELATED WORK

LITERATURE SURVEY

Sr. No	Paper Name	Author	Year	Disadvantage
1.	"Lossy Compression and Iterative Reconstruction for Encrypted Image"	X.Zhang	Feb 2006	Loss of data in encrypted image
2.	"Commutative Encryption and Watermarking in Video Compression"	Z.Ren	Feb 2009	Time consuming
3.	"Composite Signal Representation for Fast and Storage-Efficient Processing of Encrypted Signals"	M.Barni	March 2010	Not suitable for large scale system
4.	"Fundamentals of computer security"	M.Joset Pierprzyk	June 2003	----------

EXISTING SYSTEM

In Exisiting system, encrypytion starts with encrypting image. When encryption has done successfully, one encryption key is generated. Then the data is hide behind the image. When image is decrypted data is visible easily.

Existing system uses these two algorithms

1. AES (Advanced Encryption Standard)
2. DES (Data Encryption Standard)

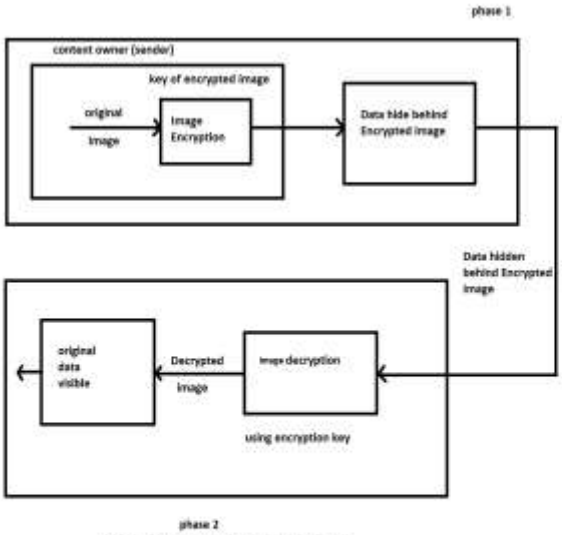

Fig 1 : Concept of Existing System

Disadvantages of Existing System

- Only single level encryption is done.
- Less percentages of data security is provided in this system.
- Data is visible easily.
- Less secure in highly confidential projects.

PROPOSED SYSTEM

In first phase we do the image encryption and generate image encryption key. Then data is encrypted and embed into image using RC4 algorithm and hiding key. Achieving both level of encryption using JSP & Servlet method. Mailed the image, encryption and data hiding keys to receiver. Receiver decrypt the image and data using that keys.

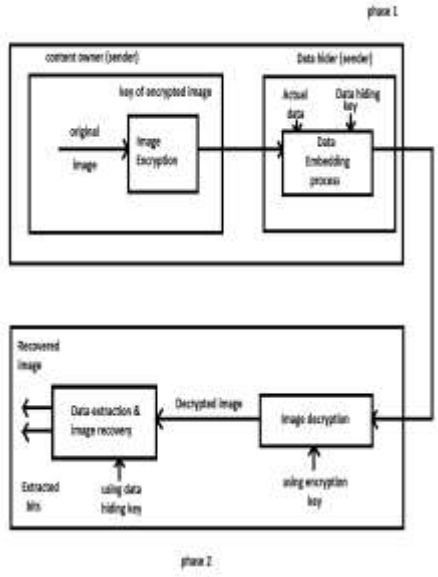

Fig 2:- Concept of Proposed sytem

SYSTEM MODULE

1) Image Selection & Encryption Module

A) Image Encryption Types

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

B) Generation of Encryption Key

Generated Encryption key value is 128 bit . Using the random function, it is generated randomly. The random function generates the random key in an uniformly distributed function.

C) Generation of Pseudo-Random Sequence

In this phase Pseudo random sequence consists of random bits generated using the encryption key. In system, RC-4 algorithm is used to create the pseudo-random sequence using the 128-bit encryption key .genrated bytes equal to the pixels & input image provided as 8-bit value. suppose 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

Text editions have been completed, then paper is ready for the template. The Duplicate template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper.Highlight all of the contents and import your prepared text in newly created file,. Your paper redy to style; use the scroll down window on the left of the MS Word Formatting toolbar. In 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 - 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 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

In proposed scheme is made up of image encryption, data embedding and data-extraction image-recovery phases. The sender encrypts the original uncompressed image using an encryption key to produce an encrypted image. Then, the 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. An 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. here data embedding only affects the LSB, a decryption and encryption key can result in an image similar to the original version [4]. 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.

4) Result Module

The test image Lena sized 512 ×512is used as the original image in the experiment. After image encryption, the eight encrypted bits of each pixel are converted into a gray value to generate an encrypted image.

ADVANTAGES

- Compared with the other algorithms, the proposed system demonstrated successful accuracy in recovering the original images
- Less chances of hacking
- More reliable
- Reduces the time & space complexity.
- More secure than other algorithm of data encryption

APPLICATION

- It will provide data security in military sites information of any country
- It will provide data security in online transaction
- It will provide security in banking transaction
- It will provide data security in social side accesing

.

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,

9) M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. G. B. Natale, and A Neri, "A commutative digital image watermarking and encryption method in the tree structured H transform domain," *Signal Processing:*