ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

An Empirical Model of Secure Data Transmission Technique with a Hybrid Approach of Cryptography, Stegnography And Rotational Analysis

Bhogi Viswakanth
M.Tech(Software Engineering),
Department Of Computer Science and Engineering,
Sarada Institute of Science Technology and Mangement, Srikakulam.

M Jayanthi Rao
Head of The Department
Department of Computer Science and Engineering,
Sarada Institute of Science Technology and Mangement, Srikakulam.

Abstract:

Today security is an important thing when we need to transmit data from one location to another safely. We are proposing an empirical model of secure data transmission technique with a hybrid approach of Cryptography, Stegnography and rotational analysis. In the initial phase data is encrypted with RSA algorithm with the help of Session key which is generated by the Key-Generation of RSA. In the second phase Cipher Data is hidden in to the cover image's LSB to form the stego image, by considering security as the optimal security parameter, In the third phase the Stego image is rotated with specific angle. At the receiver end, the image is de-rotated and the cipher information from the LSB is retrieved and the cipher information is decrypted with session key.

This scheme achieves lossless recovery and is difficult to decrypt by the attackers. In other words, content owner encrypts the original uncompressed image using an encryptionkey. Then, a data-hider may compress the least significant bitsof the encrypted image using a data-hiding key to create asparse space to accommodate some additional data. Using datahiding key the receiver can extract additional data even thereceiver has no information about the original image content. Using the decryption key the receiver can extract data toobtain an image similar to the original one, but cannot extractthe additional data. If the receiver has both the data-hiding keyand the encryption key, the receiver can extract the additionaldata and the original image without any loss.

Keywords:

Image encryption, image recovery, reversible data hiding, Keys, Privacy Protection, Data Extraction

Introduction:

In computer science, secure transmission refers to the transfer of data such as confidential or proprietary information over a secure channel. Many secure transmission methods require a type of encryption. The most common email encryption is called PKI. In order to open the encrypted file an exchange of keys is done.

Many infrastructures such as banks rely on secure transmission protocols to prevent a catastrophic breach of security. Secure transmissions are put in place to prevent attacks such as ARP spoofing and general data loss. Software and hardware implementations which attempt to detect and prevent the unauthorized transmission of information from the computer systems to an organization on the outside may be referred to as Information Leak Detection and Prevention (ILDP), Information Leak Prevention (ILP), Content Monitoring and Filtering (CMF) or Extrusion Prevention systems and are used in connection with other methods to ensure secure transmission of data.

Existing System :

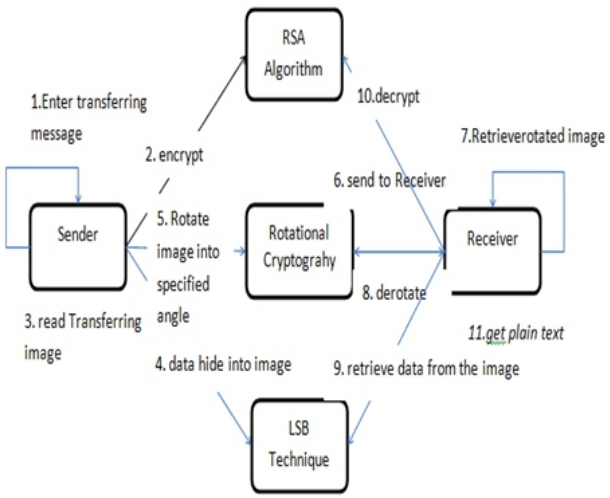
As our initial research starts with the different types of attacks, mainly classified as Active attacks

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

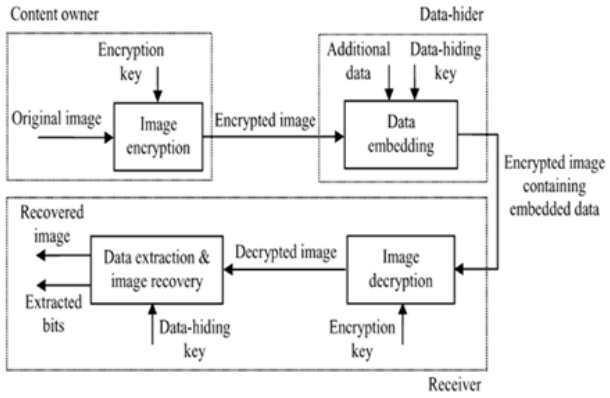
(Interruption, modification, fabrication) and passive attacks(Interception) during the transmission of data, Cryptography introduced to convert the formatted text to unformatted text through the various cryptographic algorithms.Now a days hackers and Attackers are also very familiar with cryptanalysis(cracking of ciphers or unformatted texts),so cryptography may not resolve the problem of security, later stegnography is introduced for hiding the data into the image,because of simple implementation issue and human eye undetectable changes.In this process we consider these two parameters i.e., cover image and the message are embeded and forms the stego image. Eventhough various cryptography and stegnographic approaches are developed, security is still an importantant research issue in the field of network security.

Proposed System:

We are proposing a hybrid approach with both cryptography and rotational visual cryptography for secure data transmission over the network. In our approach, initially the sender converts the plain text to cipher text with RSA algorithm. RSA algorithm requires a key for the process of encryption and decryption, which can be achieved by the key generation procedure in RSA . After the session key generation, the sender converts the plain text to cipher text by RSAalgorithm . The cover image is selected and is converted into binary format and the cipher text is embeded into the LSB of the binary format of the image which forms the stego image. The stego image is rotated by some specific angle and is sent to receiver. The reverse process is done at the receiver end. The entire process is shown in architectural figure1



Architecture:



Key generation:

RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated the following way:

1.Choose two distinct prime numbers p and q.

• For security purposes, the integers p and q should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primality test.

2.Compute n = pq.

• n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.

3.Compute $\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1) = n - (p + q - 1)$, where φ is Euler's totient function.

4.Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e., e and $\varphi(n)$ are coprime.

• e is released as the public key exponent.

• e having a short bit-length and small Hamming weight results in more efficient encryption – most commonly$2^{16} + 1 = 65,537$. However, much smaller values of e (such as 3) have been shown to be less secure in some settings.[5]

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

5.Determine d as d e–1 (mod φ(n)); i.e., d is the multiplicative inverse of e (modulo φ(n)).

• This is more clearly stated as: solve for d given de 1 (mod φ(n))

• This is often computed using the extended Euclidean algorithm. Using the pseudocode in the Modular integerssection, inputs a and n correspond to e and φ(n), respectively.

• d is kept as the private key exponent.

The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulusn and the private (or decryption) exponent d, which must be kept secret. p, q, and φ(n) must also be kept secret because they can be used to calculate d.

• An alternative, used by PKCS#1, is to choose d matching de 1 (mod λ) with λ = lcm(p − 1, q − 1), where lcm is theleast common multiple. Using λ instead of φ(n) allows more choices for d. λ can also be defined using the Carmichael function, λ(n).

• The ANSI X9.31 standard prescribes, IEEE 1363 describes, and PKCS#1 allows, that p and q match additional requirements: being strong primes, and being different enough that Fermat factorization fails.

Encryption:

Alice transmits her public key (n, e) to Bob and keeps the private key d secret. Bob then wishes to send message M to Alice.

He first turns M into an integer m, such that 0 ≤ m < n by using an agreed-upon reversible protocol known as a padding scheme. He then computes the ciphertext c corresponding to

$$c \equiv m^e \pmod{n}$$

This can be done efficiently, even for 500-bit numbers, using Modular exponentiation. Bob then transmits c to Alice. Note that at least nine values of m will yield a ciphertext c equal to m,but this is very unlikely to occur in practice.

After encryption of transmitting data the sender will put cipher data into image using LSB Technique.

LSB Approach:

LSB (Least Significant Bit) substitution is the process of adjusting the least significant bit pixels of the carrier image. It is a simple approach for embedding message and the image. The Least Significant Bit insertion varies according to number of bits in an image. For an 8 bit image, the least significant bit i.e., the 8 th bit of each byte of the image is changed with the bit of cipher text. For a 24 bit image, the colors of each component like RGB (red, green and blue) are changed. LSB is effective in using BMP images since the compression in BMP is lossless.

ROTATIONAL ANALYSIS:

Rotational Analysis is a new approach where the image is rotated with an angle instead of sending it directly. In our approach, after hiding the data in the image, it is rotated with a specific angle by the sender and is sent to the receiver. In the reverse process, receiver derotates the image with the same angle, extracts the cipher information from the stego image. The cipher data again to send to decryption process RSA Algorithm. The decryption process RSA as follows.

Decryption:

Alice can recover m from c by using her private key exponent d via computing

$$m \equiv c^d \pmod{n}$$

Given m, she can recover the original message M by reversing the padding scheme.

Conclusion:

We are concluding our research issue with empirical approach of data hiding through rotational visual cryptography. Our experimental result shows an efficient performance results than the traditional approach with hybrid mechanism of cryptography, stegnogrpahy and rotational visual cryptography In this paper we are proposed concept of key generation,encryption and decryption process for convert data into cipher format.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

We are using RSA Algorithm for key generation, encryption and decryption of transferring data. In this paper we are using another technique for data hide into image LSB and rotational cryptography for rotate image into specified angle.

References:

[1] Xinpeng Zhang, Separable Reversible Data Hiding in Encrypted Image, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 2, APRIL 2012.

[2]MazharTayel, HamedShawky, Alaa El-Din Sayed Hafez, "A New Chaos Steganography Algorithm for Hiding Multimedia Data" Feb. 19 22,2012 ICACT2012.

[3] AkashMandal, Chandra Prakash, Mrs. ArchanaTiwari, "Performance Evaluation of Cryptographic Algorithms: DES and AES," IEEE Trans.on Electrical, Electronics and Computer Science, 2012.

[4] Lokesh Kumar, "Novel Security Scheme for Image Steganography using Cryptography Technique", Volume 2,Issue 4, April 2012.

[5] Komel Patel, SumitUtareja, Hitesh Gupta, "A Survey of Information Hiding Techniques", Volume 3, Issue 1,Jan 2013, IISN: 2250-2459.

[6] B. Padmavathi, S. RanjithaKumari, "A survey on-Performance Analysis of DES, AES and RSA algorithm along with LSB Substitution Technique", Volume 2, Issue 4, April 2013,ISSN: 2319-7064.

[7] P. Mohan Kumar, Dr. K. L. Sunmuganathan, "A Reversible High Embedding Capacity Data Hiding Technique for Hiding Secret Data in Images", vol. 7, No. 3, March 2012.

[8] 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.

[9] 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.

[10] X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," IEEE Trans. Inform. Forensics Security, vol. 6, no. 1, pp. 53–58, Feb. 2011.

[11] T. Bianchi, A. Piva, and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted domain," IEEE Trans. Inform. Forensics Security, vol. 4, no. 1, pp. 86–97, Feb. 2009.

[12] 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.

[13] N. Memon and P. W. Wong, "A buyer-seller watermarking protocol," IEEE Trans. Image Process., vol. 10, no. 4, pp. 643–649, Apr. 2001.

[14] M. Kuribayashi and H. Tanaka, "Fingerprinting protocol for images based on additive homomorphic property," IEEE Trans. Image Process., vol. 14, no. 12, pp. 2129–2139, Dec. 2005.

[15] M. Deng, T. Bianchi, A. Piva, and B. Preneel, "An efficient buyer-seller watermarking protocol based on composite signal representation," in Proc. 11th ACM Workshop Multimedia and Security, 2009, pp. 9–18.

Author Details :

Bhogi.viswakanthis

student in M.Tech(software engineering) in Sarada Institute of Science Technology and Management, Srikakulam. He has received his B.Tech(CSE) from Sarada Institute of Technology And Management(SISTAM), Srikakulam. . His interesting areas are Data Mining, Networking.

JayanthiRaoMadina

is working as a HODin Sarada Institute of Science, TechnologyAnd Management(SISTAM), Srikakulam,Andhra Pradesh. He received his M.Tech(CSE) from Aditya Institute ofTechnology And Management(AITAM),Tekkali. Andhra Pradesh. His researchareas include Image Processing, Computer Networks, DataMining, Distributed Systems. He published six papers in international journals and he attended for three conferences.