© UNIVERSAL RESEARCH REPORTS | REFEREED | PEER REVIEWED
ISSN : 2348 - 5612 | Volume : 05 , Issue : 01 | January – March 2018

IMPLEMENTATION OF PICTURE KEY ENCRYPTION USING ENHANCED TECHNOLOGY

[1]Neha Agarwal, [2]Priyanka
[1]Research Scholar, [2]Assistant Professor, Department of CSA
Chaudhary Devi Lal University

Abstract: There are lots of challenges to existing network security. Images are usually represented in two dimensions form. Several encryption techniques are used & applied in case of image encryption. It is inconvenient to encrypt or decrypt picture directly because picture are large in size. In this research the enhancement of picture key has been performed. Here in this paper we have discussed the Encryption techniques DES and RSA along with their algorithms. The tools and technology used in research have been discussed. The Implementation and scope of research has been discussed at the end.

ISSN : 2348-5612 © URR

Keywords: RSA, RPT, DES, ENCRYPTION, DECRYPTION, JAVA

[1] INTRODUCTION

There are lots of challenges to existing network security. First threat is from hacker person who hacks data in unauthentic way. In order to secure data from being hacked usually firewall & virtual private network are used. But if hackers are successful in his objective then data should be converted to non understandable form from plane text.
There are lot of challenges is taken into account while encrypting images:
The foremost issue is that similar methods are used to encode picture data as for text. Images are generally represented in 2-Dimensions form. They should be first converted into 1-Dimension form before enciphering. Various encryption techniques could be used & applied on 1-Dimension. Since picture is large, it is inconvenient to encrypt or decrypt picture directly. Due to extraordinary features of a picture it becomes tough to apply an encoding scheme on it. Chief feature of a picture is that it allows a bit of distortion. A small distortion in picture compression turns encryption in another way.

The size of compressed picture is large enough. Thus they cannot be encrypted by same method as for text. This is also inconvenient to decrease or reduce size of picture before enciphering.
Problem also depends on techniques or parameters that are considered as candidate for design of encryption techniques which are good for practical use.

[2] ENCRYPTION TECHNIQUES

In this section we have discussed encryption techniques.

Data Encryption Standard - Symmetric Key Cryptography

1. In first step, 64-bit plain text block is handed over to an Initial permutation function.
2. The Initial Permutation is performed on plain text.
3. Next, Initial Permutation produces two halves of permuted block; say Left plain text (LPT) & Right Plain Text (RPT).
4. Now, each of LPT & RPT goes through 16 rounds of encryption process.
5. In end, LPT & RPT are rejoiced & a FINAL Permutation (FP) is performed on combined block.
6. The result of this process produces 64-bit cipher text.

RSA (Rivest, Shamir, Adleman) Asymmetric Key Cryptography

1. Choose two large prime numbers P & Q.
2. Calculate N = P * Q.
3. Select public key (i.e. Encryption key) E such that it is not a factor of (P-1) & (Q-1).
4. Select private key (i.e. decryption key) D such that following equation is true:

i. (D * E) mod (P-1) * (Q-1) = 1

5. For encryption, calculate cipher text CT from plain text PT as follows: CT = PTE mod N.
6. Send CT as cipher text to receiver.
7. For decryption, calculate plain text PT from cipher text CT as follows: PT = CT^D mod N

[3] TOOLS AND TECHNOLOGY USED

Java is considered as a programming language as well as computing platform. It was released by Sun Microsystems in 1995. Lots of applications & websites are there that do not work unless Java is installed. Java is known as fast, secure, & reliable programming language. It has been in used from laptops to data centers, cell phones to Internet & Video game consoles to supercomputers. Java is known as a general purpose & high-level programming language that has been developed by Sun Microsystems. OAK was first name of Java. It had been designed for handheld devices as well as set-top boxes. Sun changed its name to Java & modified language in order to take benefits of burgeoning World Wide Web.

In 2009 Oracle Corporation has acquired Sun Microsystems & they took its ownership of two key Sun software assets that are Java & Solaris. Java code could run on several platforms such as

1. Windows
2. Linux
3. Sun Solaris
4. Mac/OS etc

[4] PROPOSED WORK

Several experiments have been conducted with this Procedure on several images. There are some steps of our proposed technique are given below:

Phase 1: Firstly we develop a particular GUI for this implementation. After that we develop a code for loading picture file in Matlab database.

Phase 2: Develop a code for encryption algorithm using wavelet with suitable key in proposed work.

When code is develop then apply on image.

Phase 3: Develop a code for compression technique using Prediction Error Clustering & Random Permutation.

Phase 4: After that we develop code for decompression & decryption process.

[5] IMPLEMENTATION

Snapshots of Key exchange problem

The various snapshots for key exchange problem are given below:-

Fig 5.1 Snapshot of Symmetric Cryptosystem

Above figure 5.1 would be first view of simulation. In this figure both approach are shown i.e. Symmetric key (Traditional approach) & Picture key (Proposed Protocol).

© UNIVERSAL RESEARCH REPORTS | REFEREED | PEER REVIEWED
ISSN : 2348 - 5612 | Volume : 05 , Issue : 01 | January – March 2018

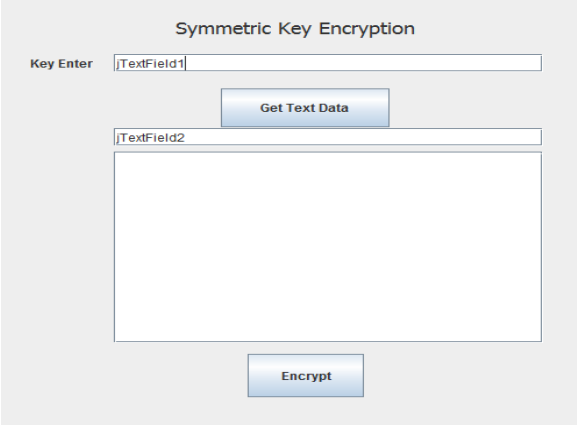

Fig 5.2 Snapshot of Symmetric Key Encryption

In above figure 5.2 we would perform symmetric key encryption i.e. traditional approach which would be performed on text message with help of key.

Fig 5.3 Snapshot of Message Encrypted

In above figure 5.3 we have taken a message **"hello how r u?"** as our plain text & then encrypted message with a key **"123456"**.

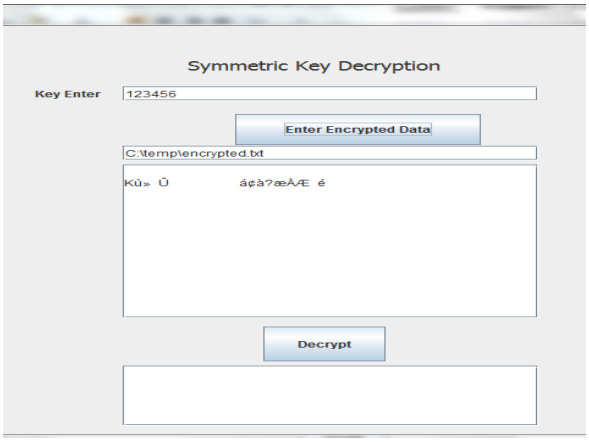

Fig 5.4 Snapshot of Symmetric Key Decryption

In above figure 5.4 we are performing decryption process. For that we are taking same key as used for encryption. Here key exchange is a big issue more over intruder could easily attack on key.

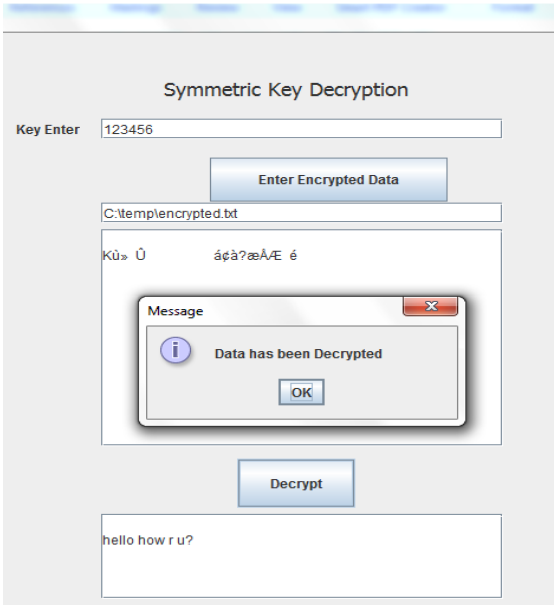

Fig 5.5 Snapshot of Message Decrypted

In above figure 5.5 we performed decryption process on encrypted data using same key & we got same plain text.

Proposed Protocol

Sender side:-

© UNIVERSAL RESEARCH REPORTS | REFEREED | PEER REVIEWED
ISSN : 2348 - 5612 | Volume : 05 , Issue : 01 | January – March 2018

Fig 5.6 Snapshot of Picture Key Cryptosystem

For proposed protocol key picture & data picture are shared between sender & receiver.

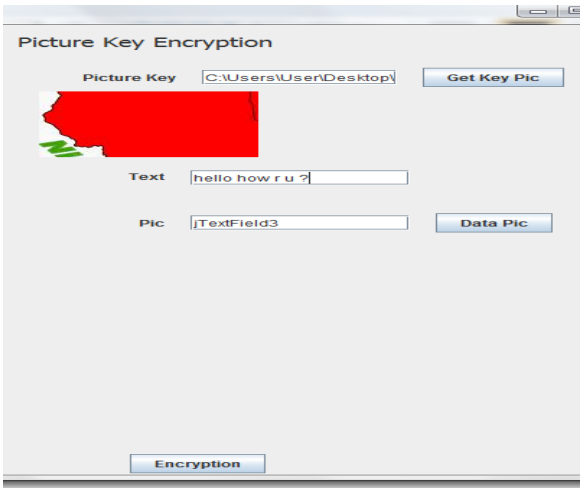

Fig 5.7 Snapshot of Message Encrypted with Shared Picture

In above figure 5.7 we have taken same message “hell how r u?” as our plain text. Plain text is encrypted using Key picture with DES.

Fig 5.8 Snapshot of Browsing of Cover Picture for Encryption

In above figure 5.8 we have taken data picture to encrypt cipher picture.

Fig 5.9 Snapshot of Encrypted Message Is Again Encrypted With Cover Picture

In above figure 5.9 cipher picture is encrypted using Data picture with help of DES. We would get resultant picture. This resultant picture would be sent to receiver.

© UNIVERSAL RESEARCH REPORTS | REFEREED | PEER REVIEWED
ISSN : 2348 - 5612 | Volume : 05 , Issue : 01 | January – March 2018

Recover side:-

Fig 5.10 Snapshot of Picture Key Decryption

In above figure 5.10 same Data picture is taken for decryption process & decryption is performed to get cipher picture.

Fig 5.11 Snapshot of Decryption of Message with Cover Picture

In above figure 5.11 same Key pictures are used for perfuming decryption on cipher picture to get plain text.

Fig 5.12 Snapshot of Decryption of Message with Shared Picture

[6] CONCLUSION

A new picture-password based key establishment algorithm is presented that use both private & public key cryptography. The proposed protocols provide a practical solution to problem of offline dictionary attack from which Seo & Sweeny protocol suffers. By customization of protocol it becomes very convenient & practical. Moreover simple text encryption/decryption suffers from problems such as confidentiality, authentication & integrity i.e. main attack is Man-in-Middle attack.

REFERENCES

1. Shobha Pati (2008) A Secure Approach to Image Encryption of color image without using key International Journal of Current Engineering & Technology
2. Chi Chang-Yanab, et al., (2008) have done a study on methods of noise reduction within a stripped image
3. Mariusz Leszczyński (2010) has worked on image preprocessing for illumination invariant face verification
4. Dr.Ch. Srinivasa Rao (2010) Analysis on Keyless Approach of Image Encryption International Journal of

Research & Computational Technology, Vol.7

5. Gamil R.S. Qaid , Sanjay N. Talbar(2012) Encryption & Decryption of Digital picture Using Color Signal" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 2, March 2012

6. P. Radhadevi1, P. Kalpana (2012) Secure Picture encryption using aes" International Journal of Research In Engineering & Technology Volume: 01 Issue: 02 Oct-2012

7. Payal SharmaDigita(2012) Image Encryption Techniques: A Review International Journal of Computing & Business Research

8. Subhajit DasAn(2013) Innovative Approach in Image Encryption Proc. of Int. Conf. on Recent Trends in Information, Telecommunication & Computing, ITC

9. Rinki Pakshwar, Vijay Kumar (2013) A Survey On Different picture Encryption & Decryption Techniques" International Journal of Computer Science & Information Technologies, Vol. 4

10. Jyotika Kapur(2013) Security using picture processing" International Journal of Managing Information Technology (IJMIT) Vol.5, No.2, might 2013

11. Umashankar Pandey (2013) Literature Survey & Performance Analysis of Image Encryption Technique Based on Chaotic Schemes International Journal of Computer Technology & Electronics Engineering (IJCTEE) Volume 3, Issue 6, December 2013

12. **Nur Amalina (2013) Enhanced Network Security System Using Firewalls ARPN**

13. Manish Kumar (2014) A first approach on an RGB image encryption Optics & Lasers in Engineering 52 (2014)

14. **Archit Uprit (2014) Network Security Using Linux/Unix Firewall**

15. Assistant Professor (2014) Unique Key Using Encryption & Decryption of Image International Journal of Advanced Research in Computer & Communication Engineering Vol. 3, Issue 10, October 2014

16. Mohammad Sajid Qamruddin Khizrai(2014) Image Encryption using Different Techniques for High Security Transmission over a Network International Journal of Engineering Research & General Science Volume 2, Issue 4, June-July, 2014

17. Ravi Prakash Dewangan(2015) Image Encryption using Random Permutation by Different Key Size International Journal of Science, Engineering & Technology Research (IJSETR), Volume 4, Issue 10, October 2015

18. Samreen Sekhon Brar(2016) Double Layer picture Security System using Encryption & Steganography"J. Computer Network & Information Security, 2016

19. Dipak Aher(2016) Novel Framework of Hyper Image Encryption Algorithm International Journal of Emerging Technologies in Engineering Research (IJETER) Volume 4, Issue 5, might (2016)

20. Shahriar Mohammadi, Reza Ebrahimi Atani, Hossein Jadidoleslamy (2011) A Comparison of Link Layer Attacks on Wireless Sensor Networks *Journal of Information Security*, 2011

21. Wajeb Gharibi & Maha Shaabi (2012) Cyber threats in social networking websites, International Journal of Distributed & Parallel Systems (IJDPS) Vol.3, No.1, January 2012

22. Tongguang Ni, Xiaoqing Gu, Hongyuan Wang, & Yu Li (2013) Real-Time Detection of Application-Layer DDoS Attack Using Time Series Analysis, Journal of Control Science & Engineering Volume 2013,

23. Hong-Ning Dai, QiuWang, Dong Li, & Raymond Chi-Wing Wong (2013) On Eavesdropping Attacks in Wireless Sensor Networks with Directional Antennas, International Journal of Distributed Sensor Networks Volume 2013,

24. Rupam, Atul Verma, Ankita Singh (2013) An Approach to Detect Packets Using Packet Sniffing, International Journal of Computer Science &

Engineering Survey (IJCSES) Vol.4, No.3, June 2013

25. Sharmin Rashid, Subhra Prosun Paul (2013) Proposed Methods of IP Spoofing Detection & Prevention, International Journal of Science & Research (IJSR), Volume 2 Issue 8, August 2013