AN EFFECTIVE TECHNIQUE FOR PREVENTING BRUTEFORCE AND TIMING ATTACK IN THE STEGANOGRAPHY

Monika (M.Tech) **Prof. Ajit Singh**

M.Tech Student **Chairperson Deptt. Of CSE & IT**

Department Of Computer Science & Engineering

BPS Mahila Vishvavidyalya, Khanpur Kalan, Sonipat.

Abstract: The present paper provides the conceptual frame technique on the XOR technique to restrict brute force and timing attack during communication .It allows data encryption in minimum time. In the first phase proposed technique provides IP authentication, and in second phase it considers the security related to session. During the third phase XOR technique provide user authentication for security. The present paper is simulating the proposed XOR technique and show how it prevents brute force and timing Attacks. Proposed technique has enhanced the security of Steganography technique. Technique has resolved the issues that were faced by traditional researches. Design secure encoding and decoding technique to enhance the protection of system would allow user to transfer data over net technique without delay and loss of data. The proposed XOR technique is more secure in all sense as it is immune to brute force attack as well as timing attack. Thus there is no possibility of such kind of attacks. The XOR based security technique has improved the performance of encryption and decryption. Additional security techniques such as IP verification restrict the attacks from hacker end.

Keywords: Steganography**,** Encryption, MATLAB, Security, Brute force, Timing.

1 Introduction

Steganography [1] is beating of a secret data stored in general message. It is retrieval of this message at target location. Steganography is enhancing cryptography [2]. It is performing this hiding encrypted data. Steganography [3] is art where messages, images or files are protected in messages.

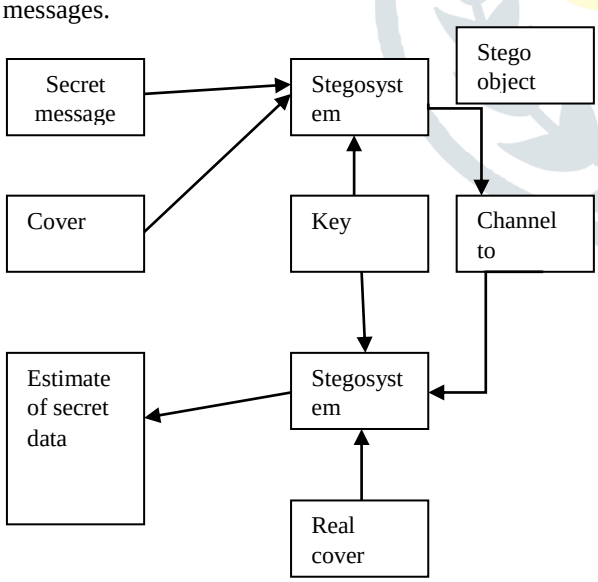

Fig: 1: Model of Steganography [1]

Cryptography [6] has been considered enciphering & deciphering of data. This process is done in secret code.
Concept of Steganography [4] has been used from long time. Benefit of Steganography [5] is that payload has been not expected by person who investigates it.

2 Existing RSA Technique

RSA has been considered first public key based cryptosystems. Generally it is applied for protect the content [7] transmission. In the cryptosystem [8], encryption key has been considered for public use. It is separate from decryption [9] key that is reserved secretly. In RSA, this irregularity is dependent on the practical complexity. It is about the factorization of multiplication of large prime numbers. There is a factoring issue. A client of RSA formulates along with publishes a public key. It is dependent on the values huge prime. Prime value must be hold secretly. Anyone may apply public key in order to encrypt [11] data. Someone having knowledge of prime numbers might be capable to decrypt data. Breaking RSA encryption [12] has been considered as RSA problem.

Requirements algorithm implementation RSA

The RSA algorithm's keys have been created the phase which is giving below:

1. Select two separate prime numbers p1 along with q1.
2. For the objective of protection, the integer's p1 along with q1 need to be selected randomly. It would be like as in magnitude. But vary in size with a small number of digits to create factoring harder.
3. Calculate nn = PQ.

- N has been considered as modulus for public along with private keys. Generally, its size, uttered in bits which are length of key.

4. Compute λ (nn) = 1cm (λ (p1), λ (q1)) = l cm (p1 − 1, q1 − 1), λ is Carmichael's totient function. Value has been considered the private.
5. Select integer iei like 1 < iei < λ (nn) along with gcd (iei, λ(nn)) = 1, for example iei along with λ(nn) are co prime.

6. Suppose dx as dx = e^{-1} (mod λ(nn)); for example dx. It has been considered modular multiplicative opposite of e (modulo λ (nn)).
1. It has been considered more visible which is declared as: solve for d allocated d·e = 1 (mod λ (nn)).
2. Ex has short bit length along with less Hamming weight output in the case of efficiency of encryption generally e = 2^{16} + 1. Thus, minimum value of e is displayed having less protection in system.
3. Ex has been declared public key promoter.
4. D has been considered private key exponent.

2.1 Equation of RSA with Example

RSA's Principle has been considered as observation. It requires the integer's e, d as well as n.

For integer mx (with 0 ≤ mx < nx):

$(mx^e)^d$=mx(mod nx)

If e,nx ,mx are known it is complicated to get d.

In addition this relation is also represented as:

$(mx^d)^e$=mx(mod nx)

p1 and q1 are prime numbers here

nx = p1xq1

λ (nx) = lcm(λ(p1), λ(q1))

= LCM (p1 − 1, q1 − 1)

λ has been considered as Carmichael's totient function.

2.2 Input for RSA encryption

Public key: (1189, 7)

Private Key: 249

Let the plaintext is 19. There is need to compute:

Cipher text = 199 mod 1189.

It has been calculated with the help of Algorithm of Repeated Squares:

Step 1:

Ciphertext=198+1%1189

Ciphertext=(198)(191)%1189

Step 2:

191=19%1189

192=192=361%1189

194=720%1189

198 = 1185 % 1189

Step 3:

Ciphertext=(198)(191)%1189

=(1185)(19)%1189

=22515%1189

= 1113 % 1189

Output of RSA encryption

So the cipher text C is 1113.

2.3 Input for RSA BASED DECRYPTION

Let this Cipher text=1113 has been received. In order to decrypt this cipher text there is need to compute:

Plaintext = 1113249 % 1189.

This is most efficiently calculated using Repeated Squares Algorithm:

Step 1:

plaintext≡1113249%1189

plaintext≡1113128+64+32+16+8+1%1189

plaintext≡(1113128)(111364)(111332)(111316)(11138)(11131)%1189

Step 2:

11131=1113%1189

11132=1020%1189

11134=25%1189

11138=625%1189

111316=633%1189

111332=1185%1189

111364=16%1189

1113128 = 256%1189

Step 3:

plaintext

=(1113128)(111364)(111332)(111316)(11138)(11131)%1189

=(256)(16)(1185)(633)(625)(1113)%1189

=2137259174400000%1189

= 19 % 1189

OUTPUT: The value of plaintext is 19.

2.4 Limitations

The RSA algorithm is very slow where huge information requires to be encrypted. It needs a third party to confirm trustworthiness of public keys. Information [15] transmitted using RSA algorithm is compromised with men in middle. This person could temper with public key based system. Finally symmetric based encryption technique along with asymmetric encryption techniques have been found useful for encryption [18].

1. The traditions technique makes the data transmission slow.
2. There are chances of cracking security of traditional technique.
3. There is lack of interactive interface in traditional technique.
4. The unauthentic packet could be transferred using present ports thus here is need of user defined port.
5. There is lack of security at session level.

3 PROPOSED XOR TECHNIQUE

The proposed XOR technique is more secure and more efficient as compare to traditional security technique. Design of Integrating to enhance the security of Steganography [12][26] technique has resolved the issues with traditional researches. Design secure encoding and decoding technique to enhance the protection of system would allow user to transfer data over nettechnique without delay and loss of data. Cryptography has been indulged in development of written codes. This code makes data secret. Cryptography performs the conversion of data in such a format which is not understandable to unauthorized user. Cryptography [15] is helps transmission of data without being decoded by unauthorized users. Information security has been utilizing cryptography on many layers. Data is not readable without decryption. Data is maintaining its integrity at the time of transmission and storage. [16]

3.1 Requirements

The basic requirements to perform XOR based encryption [14] are data to be encrypted and key to encrypt the data.

Data: The information that is to be encrypted before transmission. The data is the content of file that needs to secure.

Key: This is the key content using which data is encrypted and decrypted. This key must be available during encryption and decryption time in order to encrypt and decrypt data.

Iteration is repetition of the encryption process again and again in order to enhance the security of data. During decryption

Process same numbers of iterations are required.

3.2 Techniqueing

The techniqueings of the proposed XOR techniques in details are given as under:

During encryption process XOR operation is performed using key n times.

Data XOR key--->encdata1

Perform bit shifting in encdata1 to produce ndata1

Repeat previous two steps n times and get data.

This data is then decrypted using XOR operation with key. The reverse operation of encryption takes place during decryption process.

3.3 Triple layered security has been proposed in this XOR technique

Step-1: Security layer 1 would be capable to modify Steganography. It is to enhance security by integrating XOR operation in it.

Step-2: Security layer 2 has been capable to drop packets from unauthentic IP addresses.

Step-3: Security layer 3 would authenticate user. It would be done by allotting login password security at application layer.

Step-4: Security is increased with the help of OTP. It formulates totally useless after a used.

In this research the designing of secure encoding and decoding technique has been made to enhance the protection of system using the concept of visual Steganography [19] [22].

3.4 XOR Based Encryption Algorithm

Encryption: The steps in encryption process using XOR are given as under:

Step:-1. Take the data D to encrypt

Step:-2. Take XOR key X to encode the data

Step:-3. Set counter count=1

Step:-4. C=D XOR X

Step:-5. IF count>9 then go to step 8 otherwise

Step:-6. Get cipher data using C=C XOR X

Step:-7. Set count=count+1 go to step 5

Step:-8. Get C as cipher text and transmit over net technique

Input value is 8 and number to perform XOR is 4

Suppose input value for XOR encryption is 8

Binary of 8 is 1000

Perform 8xor4

1000x0100

=1100

The encrypted data is now 1100=12

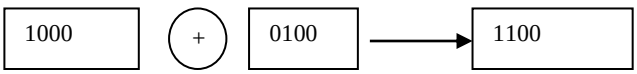

Fig 2 Output of XOR Encryption

3.5 Xor Based Decryption Algorithm

Decryption: The steps in decryption process using XOR are given as under:

Step:-1. Take the data C to Decrypt

Step:-2. Take XOR key X to decode the data

Step:-3. Set counter count=1

Step:-4. D=C XOR X

Step:-5. IF count>9 then go to step 8 otherwise

Step:-6. Get cipher data using D=D XOR X

Step:-7. Set count=count+1 go to step 5

Step:-8. Get D as normal text.

Input for XOR decryption

Input is **1100** for XOR decryption

1. 1100 would be again perform XOR with 100
2. 1100 XOR 0100 = 1000 (8)

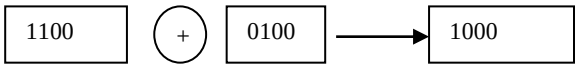

Fig 3 Output for XOR decryption is **8**

The use of XOR operator has enhanced the security of net technique. XOR key would encrypt data more efficiently as compare to traditional algorithm. The encoding and decoding process would depend of XOR key.

It is clear that from the above XOR based technique enhance the security of steganography. In additional advantage is:

1. The Proposed technique makes the data transmission fast.
2. There are little chances of cracking security of proposed technique.
3. There is presence of Graphical user interface to make interactive interface in proposed technique.
4. The unauthentic packet could not be transferred using present ports as here we have specified user defined port.
5. Session level has been provided in proposed technique.

3.6 Brute force techniqueing in case of XOR Based Encryption

There the discussion has been made how Brute force is not techniqueing in case of XOR based encryption techniques. The actual value is operated with key value and brute force technique has been applied to access data in unauthentic way.

Example:

Input value is 8 and number to perform XOR is 4

1. Suppose input value for XOR encryption is 8
2. Binary of 8 is 1000
3. Perform 8xor4
4. 1000xor0100=1100

The encrypted data is now 1100=12

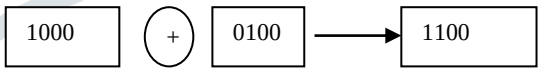

Fig 4 Output of XOR Level1 Encryption

The encrypted data is now 1100=12 would be XOR by different key 5

12xor5

1100 XOR 0101 =1001

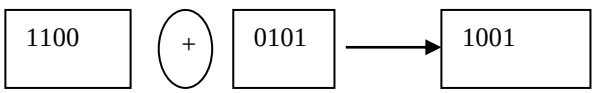

Fig 5 Output of XOR Level2 Encryption

Input for XOR decryption level 1

1. Input is **1001** for XOR decryption
2. 1001 would be again perform XOR with 101

3. 1001 XOR 0101 = 1100 (12)

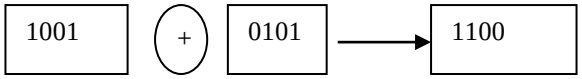

Fig 6 Output for XOR decryption is 12

Input for XOR decryption level 2

1. Input is **1100** for XOR decryption
2. 1100 would be again perform XOR with 100
3. 1100 XOR 0100 = 1000 (8)

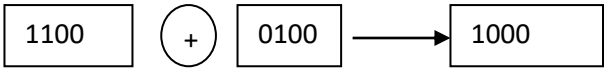

Fig 7 Output for XOR decryption is 8

XOR based security cannot be broken using Brute force attack as no any single reverse algorithm could break the security.

Timing attack is NOT technique in proposed XOR based encryption

1. SUPPOSE A=65→ 1000001
2. Perform level1 XOR with 8=0001000
3. 1000001 XOR 0001000=1001001==→73 →I
4. Perform level2 XOR with 6=0000110
5. 1001001 XOR 0000110=1001111==→79 →O

In order to mitigate this timing attack user have to change code so that it takes a fixed amount of time regardless of what the inputs are.Thus Above timing attack does not technique in proposed techniques as the representation of decrypted data is modified during next data transmission. As at the time of new session new key is used and the same encrypted data would be different during all transmissions

4. PERFORMANCE COMPARISONS OF EXISTING RSA TECHNIQUE AND PROPOSED XOR TECHNIQUE

In this section the comparative analysis of existing and proposed technique has been made. Case 1 discusses the performance of traditional RSA technique and proposed XOR technique [15] in case of brute force attack. In this simulation no of packets have been transferred using existing RSA and proposed XOR technique. The list of packets influenced in case of both has been represented in following table. Here the minimum packets have been influenced in case of proposed XOR technique [16]. Thus the performance of proposed XOR technique is better than existing RSA techniques in case of brute force attack. In other words we could say that proposed XOR technique is more immune to attack that is brute force based as compare to existing RSA technique [17].

Case 1

4.1 Comparative Analysis of Traditional RSA Technique and Proposed XOR Technique in case of Brute Force

Here discussion has been made how Brute force is not techniqueing in case of XOR based encryption technique. The actual value is operated with key value and brute force technique has been applied to access data in unauthentic way. It has been found that proposed xor technique is more secure as compared to traditional RSA technique.

No of packets	Traditional RSA	Proposed XOR
100	6	1
200	8	2
300	12	4
400	15	6
500	22	9
600	31	13
700	42	18
800	51	23
900	63	28
1000	72	32

Table 1 comparative analysis of traditional RSA and proposed XOR technique in case of brute force attack

The above table is representing the number of packets influenced by brute force attack in case of traditional RSA and Proposed XOR technique. The Table is representing the number of packets influenced in case of proposed XOR technique[23] is less as compare to Traditional RSA. Thus it is concluded that the Proposed XOR more immure to brute force attack as compare to traditional RSA.

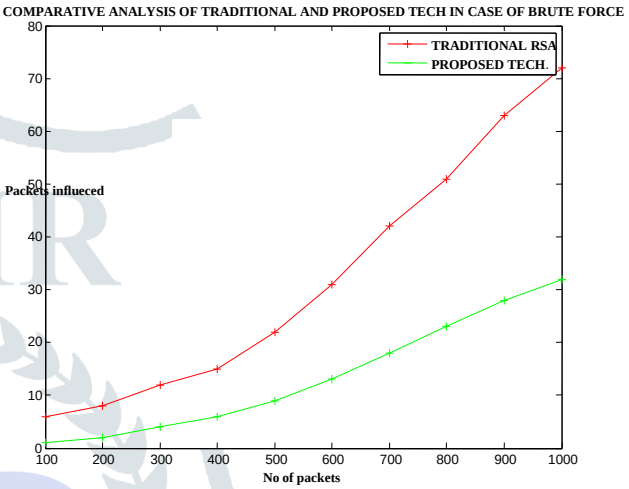

Fig 3 comparative analysis of traditional and proposed technique in case of Brute force attack

Case 2

4.2 Comparative Analysis of Traditional RSA and Proposed XOR Technique in case of Timing Attack

It has been made how timing attack is not technique in case of XOR based encryption technique. The actual value is operated with key value and timing attack technique has been applied to access data in unauthentic way. It has been found that proposed technique is more secure as compared to traditional.

No of packets	Traditional RSA	Proposed XOR
100	7	2
200	10	4
300	15	5
400	21	8
500	29	10
600	39	14
700	49	19
800	62	25
900	72	30
1000	83	35

Table 2 comparative analysis of traditional and proposed technique in case of timing attack

The above table is representing the number of packets influenced by timing attack in case of traditional RSA and Proposed XOR technique. The Table is representing the

number of packets influenced in case of Proposed XOR technique is less as compare to Traditional RSA. Thus it is concluded that the proposed XOR technique is more immure to timing attack as compare to traditional RSA.

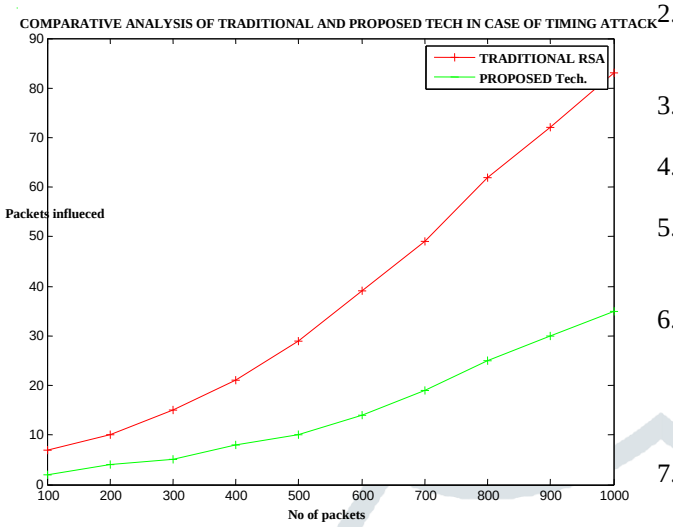

Fig 4 comparative analysis of traditional RSA and proposed XOR technique in case of timing attack

5 APPLICATION AREAS

Application area of research has been Steganography [20] along with security of nettechnique. In this research proposed XOR technique has analyzed perfect algorithm. This algorithm would embed data in graphic file [21]. This would be done using Steganography approach. It is providing good security pattern in order to transfer data over nettechnique. In present scenario, term Hacking is usually listened by us. Hacking has been considered as an unauthorized access of data. This data might be stored during the information transfer. Such issues are usually known as Steganalysis with respect to Steganography [24]. Steganalysis has been considered as a process in which a steganalyzer [25] breaks object to access secret information. Thus whatever be methodology would be made in future, security level related with that need should be considered. In dual Steganography, Steganography with Cryptography [30] could be solution in future for such issues.

6 FUTURE SCOPES AND CONCLUSION

The scope of project has been limited to unauthorized access. Research would give better security at the time of message transmission. In order to fulfill needs, it is using simple as well as general methods of Steganography. The proposed technique is more secure in all sense as it is immune to brute force attack as well as timing attack. The XOR based security has been improved the performance of encryption and decryption. Additional security techniques such as IP verification restrict the attacks from hacker end. The use of such security techniques has improved the security from hacker as well security from cracker. Here the cracker is the person who tries to decrypt data without authentications. The data hacking has been restricted by use of IP address verification and the cracking has been restricted by use of XOR based security system.

REFERENCE

1. Erin Michaud(2003) “Current Steganography Tools and Methods”, SANS Institute 2003, As part of GIAC practical repository
2. Dipti Kapoor Sarmah1, Neha Bajpai (2009) “ Proposed System for data hiding using Cryptography and Steganography ”,
3. Dragoş Dumitrescu1, Ioan-Mihail Stan1, Emil Simion (2009) “ Steganography techniques”,
4. George Abboud (2010) Steganography & Visual Cryptography in Computer Forensics 2010
5. Masoud Nosrati, Ronak Karimi (2011) “An introduction to Steganography methods”, World Applied Programming, Vol (1), No (3), August 2011. 191-195
6. Pranab Garg, Jaswinder Singh Dilawari (2012) “A Review Paper on Cryptography and Significance of Key Length”, International Journal of Computer Science and Communication Engineering IJCSCE Special issue on “Emerging Trends in Engineering” ICETIE 2012
7. Pria Bharti, Roopali Soni (2012) “ A New Approach of Data Hiding in Images using Cryptography and Steganography ”, International Journal of Computer Applications Volume 58– No.18, November 2012
8. Nitin Jirwan, Ajay Singh, Dr. Sandip Vijay (2013) “Review and Analysis of Cryptography Techniques”, International Journal of Scientific & Engineering Research Volume 4, Issue3, March-2013
9. Priyanka Bubna, Anshula Panchabudhe, Pallavi Choudhari (2017) “Review on Implementation Visual Cryptography & Steganography for Secure Authentication”, International Research Journal of Engineering and Technology Volume: 04 Issue: 02 | Feb -2017
10. Rakhi1, Suresh Gawande (2013) “A Review on Steganography Methods”, IJARE, Vol. 2, Issue 10, October 2013
11. Anjula Gupta Navpreet Kaur Walia (2014) “ Cryptography Algorithms: A Review”, 2014 IJEDR | Volume 2, Issue 2 |
12. Vikas Yadav Vaishali Ingale Ashwini Sapkal and Geeta Patil (2014) “Cryptographic Steganography ”, Computer Science & Information Technology
13. Mr. Falesh M. Shelke1, Miss. Ashwini A. Dongre (2014) “Comparison of different techniques for Steganography in images”, International Journal of Application or Innovation in Engineering & Management, Volume 3, Issue 2, February 2014
14. Priyanka B. Kutade, Parul S. Arora Bhalotra (2015) “A Survey on Various Approaches of Image Steganography ”, International Journal of Computer Applications Volume 109 – No. 3, January 2015
15. S.M.Poonkuzhali1 , M.Therasa (2015) “Data Hiding Using Cryptography in case of Secure Transmission”, IJARC, Vol. 4, April 2015
16. Pradnya S. Nagdive (2015) Visual Cryptography & Steganography : A Review International Journal of Advance Research in Computer Science & Management Studies Volume 3, Issue 1, January 2015
17. S. R. Navale1 , S. S. Khandagale, R. A. Malpekar3, Prof. N. K. Chouhan4 (2015) Approach for Secure Online transaction using Visual Cryptography & Text Steganography International Journal of Engineering Research & Technology (IJERT) Vol. 4 Issue 03, March-2015
18. Souvik Roy et al, “Online Payment technique with Steganography along with cryptography”, IEEE Students’

Conference on Electrical, Electronics and Computer Science,2014

19. Sana Shiva, A.Hari Teja (2015) Secure E-marketing Using Steganography & Emergence of Cryptography Journal of Computer Science & Information Technology IJCSMC, Vol. 4, Issue. 1, January 2015, pg.532 – 538
20. Archana.O.Vyas, Sanjay.V. Dudul (2015) "An Overview of Image Steganographic Techniques", International Journal of Advanced Research in Computer Science, Volume 6, No. 5, May - June 2015
21. K.S.Seethalakshmi (2016) "Use of Visual Cryptography and Neural Nettechniques to Enhance Security in Image Steganography ", IOSR Journal of Computer Engineering Special Issue - AETM'16
22. Priyanka More, Pooja Tiwari, Leena Waingankar, Vivek Kumar,A. M. Bagul (2016) Online Payment System using Steganography & Visual Cryptography, International Journal of Computer Engineering In Research Trends, Volume 3, Issue 4, April-2016, pp. 157-161
23. A. Joseph Amalraj1, Dr. J. John Raybin Jose (2016) "A Survey Paper on Cryptography Techniques", IJCSMC, 2016
24. C.P.Sumathi, T.Santanam and G.Umamaheswari (2013) "Study of different Steganographic techniques for information hiding", IJCS & Engineering Survey Vol.4, No.6, December 2013
25. Anjali Tiwari, Seema Rani Yadav, N.K. Mittal(2014) "A Review on Different Image Steganography Techniques", International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 7, January 2014
26. Odai M. Al-Shatanawi and Nameer N. El. Emam (2015) "A new image Steganography algorithm based On mlsb method with random pixels Selection", International Journal of Nettechnique Security & Its Applications (IJNSA) Vol.7, No.2, March 2015
27. Thiyagarajan, P. Venkatesan, V.P. Aghila, G. "Anti-Phishing Technique using Automated Challenge Response Method", in Proceedings of IEEE- International Conference on Communications and Computational Intelligence, 2010.
28. N. Chou, R. Ledesma, Y. Teraguchi, and D. Boneh, ‚Client-side defense against web-based identity theft,' in Proc. 11th Annu. Netw. Distribut. Syst. Secure. Symp, San Diego, CA, Feb. 2005.
29. Anthony Y. Fu, Liu Wenyin, "Detecting Phishing Web Pages with Visual Similarity Assessment Based on Earth Mover's Distance (EMD)",IEEE Transactions on Dependable and Secure Computing, v 3,n 4, October/December 2006.
30. Souvik Roy et al, "Online payment system with steganography along with cryptography," Proceeding of IEEE Students' Conference on Electrical, Electronics and Computer Science , Jadavpur University, Kolkata-700032, India, 2014.