# Encryption and Decryption Using Hybrid Cryptography Techniques and Multi-level Steganography

**Shubhankar Saxena, Anushka Sharma**

***Abstract*: Data Encryption, in the present time, is used to deter malicious parties from accessing sensitive data, allowing the access to only authorized parties as it uses the key to safeguard the sensitive information to be transferred. Various cryptography techniques are used to maintain confidentiality and integrity of the data, and this paper proposes the hybrid scheme of using four layers of encryption including steganography to safeguard the authenticity of the information to be transferred. In this paper, three conventional key cryptography algorithms, which are Fibonacci series, XOR cipher and PN sequence encryption, are used along with RSA cryptography which is a public key cryptography algorithm. In addition to it, steganography technique is also used in the last two layers of our proposed model. Firstly, the whole of the encrypted string, obtained after the above cryptography algorithms, is hidden inside the first image. Now this encrypted host image is further hidden inside another image by using one bit LSB algorithm. This model offers the double security of the data as here the data is not only encrypted but also hidden in an image which again is hidden inside another image making it very hard even to detect the data.***

***Index Terms*: Cryptography, Encryption, Decryption, Fibonacci series, LSB, PN sequence, RSA, steganography, XOR cipher.***

## I. INTRODUCTION

In the modern world, a lot of digital information, in the form of text, audio, video, etc., is being transmitted through various sources over the communication system. It becomes really imperative to develop a model which allows the lossless transfer of data in as secure way as possible. So, to make the secure transfer of data various cryptography techniques and digital watermarking techniques have been introduced. Cryptography allows two persons or specific parties to exchange information secretly in a secure way so that the unauthorized parties do not gain access to the original data. The data to be sent from one party to the other is altered using various ciphering techniques, and the authorization is given only to the party which has the necessary key to alter the encrypted message to the original state. There are many encryption techniques which are highly advanced but even the simpler algorithms provide help in the secure transmission of the data. Cryptography is the process which involves the conversion of primary data known as plain text, to a jumbled form known as cipher text, using a unique confidential key [1]. The process to retrieve back the original message is called decryption. Cryptography algorithms are broadly categorized as conventional key algorithm or the secret key algorithm and public key algorithm. Conventional key algorithms include Advanced encryption standard (AES), Data encryption standard (DES), Fibonacci series and PN sequence encryptsion, XOR cipher. Public key cryptography includes algorithms like RSA and Hill cipher. The emergence of steganography has played a major role in the secure transmission of data [2]. Steganography is a technique which enables to hide the data inside an image. This data may be any text message or any other image. Thus, it becomes very tedious for the third party even to detect whether the image contains any data or not and thus provides a higher level of security. There are various techniques using which image watermarking can be done [3] like one bit LSB, two bit LSB, three bit LSB techniques, etc.

## II. PROPOSED WORK

For the very first layer of encryption in our hybrid model which consists of different cryptography techniques and steganography, as shown in Fig 1, the text message is divided into two segments. Fibonacci series encryption [4] is used in a unique way on the first segmented part of the text, while the other segment ciphering is done using the RSA encryption algorithm [5]. The use of Fibonacci series for ciphering used here is quite distinct than what is usually done which further enhances the security of the data. Here, the elements of the Fibonacci series are added to the ASCII values of each symbol present at odd index and are subtracted from those present at the even index, thereby increasing the complexity of the encryption.

The Fibonacci encrypted layer is then segmented further into two segments. Another layer of ciphering is done using XOR ciphering technique [6] on one of the parts, which generates random key and to match with the correct one whilst using PN sequence ciphering [6] is done on the second segmented part on the first layer of Fibonacci encrypted layer.

Further, the watermarking encryption using one bit LSB technique is used to store the double encrypted message, along with the RSA encrypted message in an image [7] [8]. Thus, steganography forms the third layer of our proposed model for secure data transfer and hence it ensures double security of the data transfer by hiding it. At the end, the one bit LSB watermarking technique [9] [10] is used to hide the above encrypted image formed on an objective image. The LSB watermarking forms the final

**Revised Manuscript Received on July 05, 2019**

**Shubhankar Saxena**, B Tech. in Electronics and Communication Engineering, Vellore Institute of Technology, Vellore, India.
**Anushka Sharma**, B Tech. in Electronics and Communication Engineering, Vellore Institute of Technology, Vellore, India.

layer of our encryption scheme and it not only ensures double security of the data but also hides it while transferring.[11] [12]

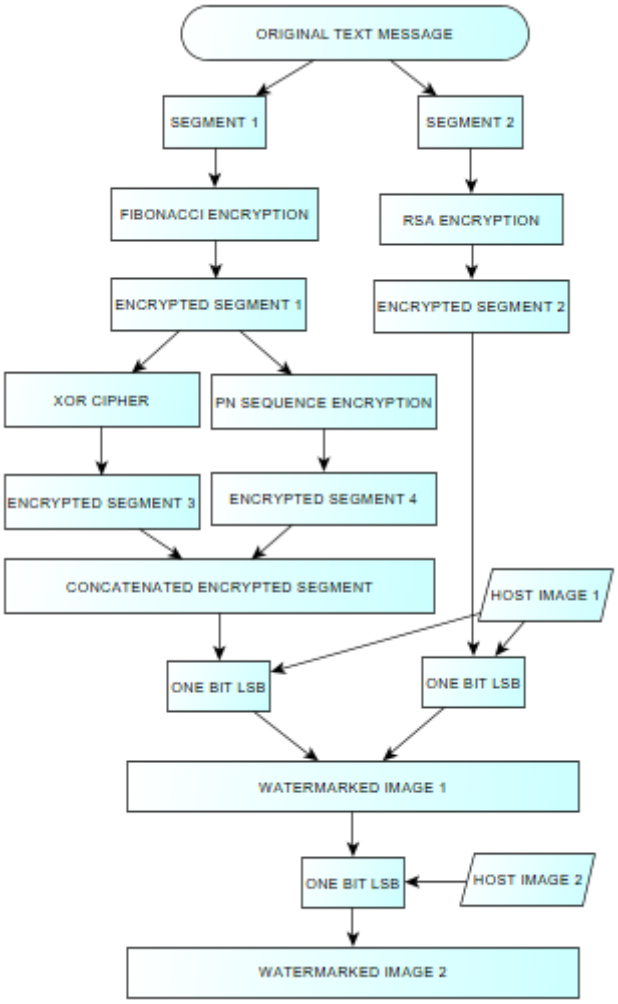


Fig 1. Block diagram for encryption

For the decryption, as shown in Fig 2, the final message is recovered back by using the decryption algorithm of the above mentioned techniques, i.e., reversing the above processes of the respective encryption algorithms, accordingly. First of all, the hidden image is retrieved back from the watermarked image two using one bit LSB technique. Now from this retrieved watermarked image one, the hidden text is recovered back using one bit LSB technique [8]. Now the segment one of the decrypted text undergoes the above mentioned cryptography techniques of XOR decryption and PN sequence decryption after which the obtained strings are concatenated which further undergoes the decryption using Fibonacci series while the segment two of the decrypted text undergoes RSA decryption [6]. After getting the two strings after the previous decryptions, these are concatenated which results in the retrieval of the original text message.

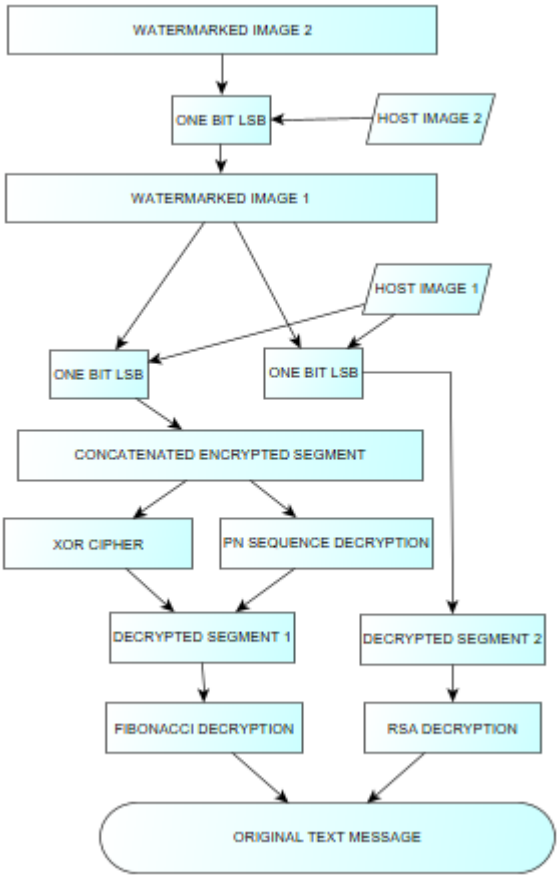


Fig 2. Block diagram for decryption

### A. *FIBONACCI SERIES ENCRYPTION AND DECRYPTION:*

1. Input the key = n, i.e., the length of the Fibonacci series.
2. Generate the Fibonacci series and store in fib.
   for i=3:n+1
   fib(i) = fib(i-1) + fib(i-2);
   end
   fib=fib(2:n+1);
3. Thus, we obtain the Fibonacci series. For encryption, reverse the text segment and store it in t1_r.
4. In a loop,
   for j = 1:n
   for i = 1:length(t1_r)
   For the odd values of the index i, add the jth term of the Fibonacci series to the ASCII value of that character. For the even values, instead of addition, subtraction is performed on the ASCII values of that character.

5) At the end of both the loop, the encrypted text obtained.
6) For decryption, create the nested loop as done in the encryption process, but here perform the reverse operations as performed in the former case.

### B. *XOR CIPHERING:*

For encryption:

1. Find the length of the text segment which is to be encrypted and store in len_t2.
   len_t2 = length(t2);

2. Now in a loop, perform bitwise XOR operation with a key to get the encrypted string.

```
for i = 1:len_t2
enc_t2(i) = bitxor(key,int8(t2(i)));
enc_t2f(i) = char(enc_t2(i));
end
```

For decryption, perform the bitwise XOR operation of the encrypted string with the unique key that was used while encrypting the segment to get the decrypted string.

*C. PN-SEQUENCE:*

1. x1 = [1 0 0];
2. Calculate the length of x1 and find the maximum number of bits that can be present in the pn sequence. len1=2^n1-1;
3. Now create the pn sequence,p1

```
for y1 = 2 : len1
x1=z1;
for i = 1 : n1
  if (i==1)
    Perform XOR operation on the second and the third
    bit and store it as the first bit of the next x1.
  else
    Store the values of the first and second bit of
    previous x1 to the second and third bit of the new x1,
    respectively.
  end
end
p1(1,y1)=z1(y1,n1);
    end
```

4. We have the pn sequence is stored in p1.

Now, perform the XOR operation of the ASCII value of each character in text with the pn sequence and store it. This is the encrypted text. The unique key can be used for the reverse process of decryption.

*D. RSA ENCRYPTION AND DECRYPTION:*

1. Find the length of the segment.
2. Select any two prime numbers p and q.
3. Find n = p*q.
4. Calculate phi = (p-1)*(q-1)
5. Through a random function, choose the value of 'e' such that gcd(p-1,e) = gcd(q-1,e) = 1.
6. Compute the value of d such that e*d ≡ 1 (mod phi).
7. Thus, the public key is (n,e) and the private key is (n,d).
8. Now, further divide the message into subtrings of length 3.
9. Store different characters (say 'p' number of characters) in variable 'a' such that each character has its own index.
10. Calculate the value of m for each substring.
    For substring1:
    t = substring1
    m(1) = (index value of 1st character of t)*p^2 + (index value of 2nd character of t)*p + index value of 3rd character of t.

    Similarly, rest of the values of 'm' can found.
11. Now, for encryption find the value of c such that c(i) = m(i)^e mod n.
12. Thus we obtain the cipher text integers in c(i). These integers are later used for the steganography for hiding this data in the image.
13. For the decryption, find m such that m(i) = c(i)^d mod n.
14. Now convert the integers in 'm' back to the block of three characters.

For retrieving the 1st substring:

a) c(1) =m(1)/(p^2). Character at the index value of c(1) is the 1st character of substring1.
b) Now rem1 = remainder of the above operation.
c) c(2) = rem1/p. Character at the index value of c(2) is the 2nd character of substring1.
   i. c(3) = remainder of the above operation and the character at its index value is the 3rd character of substring1.

The above step can be extended to obtain all the substrings.

*E. ONE BIT LSB:*

1. Resize the host image1 to the grayscale if required and convert the encrypted text to its binary format.
2. Now, initialize output image = input image.
3. Create a nested loop for traversing through all the pixels.
   a) In a loop, convert each pixel value to its binary equivalent.
   b) Get the next bit of the encrypted string bitwise, which has to be embedded.
   c) Let c = 0
   d) Now using XOR operation, compare the bit of the string and the LSB of the pixel. If they are same, then c = 0 else c = 1.
   e) Now, output = input pixel value + c
4. The process continues until the whole of the encrypted message gets embedded in the image to give an invisible watermarked image. This is the Stego image 1 which is hidden inside another image.
5. Now to embed this image in the host image 2, the former is converted to a binary image.
6. And again the whole of the above process is repeated, this time with the Stego image 1 as the message, to get the final invisible watermarked image 2 which now has the hidden text message embedded in it, secured by various layers of encryption.

This Stego image2 is send by the sender.

## III. OBSERVATIONS

. The encrypted message at the end of each layer is obtained, and the example herewith will explain further:

1. Input message from the sender: 'Let us write'
2. At the very first, the string is segmented into t1 and t2:
   t1 ='Let us'
   t2 =' write'
3. The first segmented part is encrypted using Fibonacci series encryption:
   The Fibonacci encrypted message for t1 is:
   fib_enc_r = 'wq$piH'
4. The other segmented part is encrypted using RSA algorithm:
   For the given example, the RSA

values for t2 would be such:
m = 752 495 545
c = 47 1901 1977

5. Now, the fibonacci encrypted message is further segmented into two:
xo1 = 'wq$'
pn1 = 'piH'
Now, the first part, i.e., xo1, is encrypted again using XOR ciphering:
xor_enc = '"$q'
The second part, i.e., pn1, is encrypted using PN sequence:
pn_enc = 'g~_'
6. Again, the XOR encrypted text, PN sequencing and RSA encrypted output is encrypted in an image. Like for the given example, we have the host image 1 as shown in Fig 3.

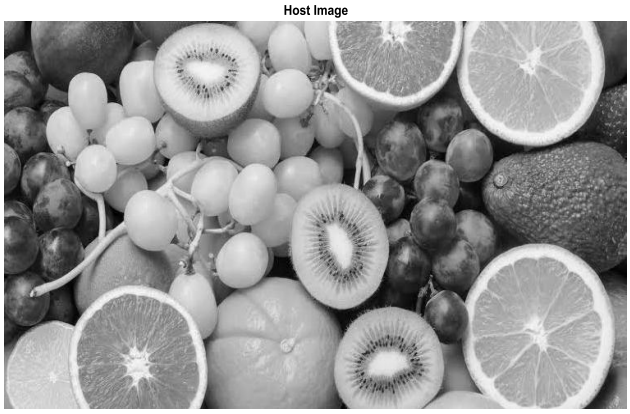

Fig 3

7. The encrypted image with the embedded text is shown in Fig 4. This image contains the XOR encrypted text, PN sequencing and RSA encrypted output. This image will be further used for the watermarking.

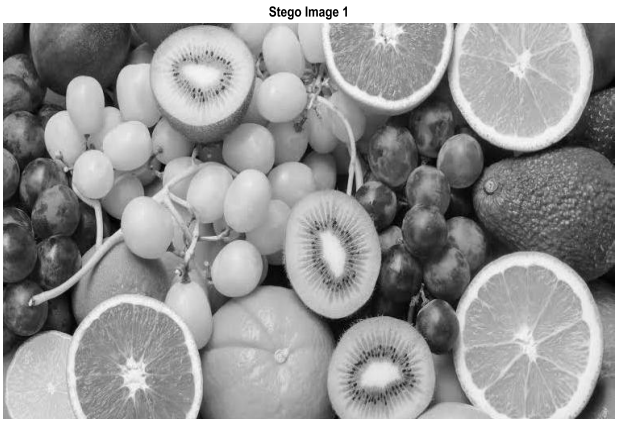

Fig 4

8. The encrypted image in Fig 4 is further converted to binary for next level of watermarking, as shown in Fig 5, which has only one bit of information for each location on which we apply the LSB watermarking technique for further encryption.

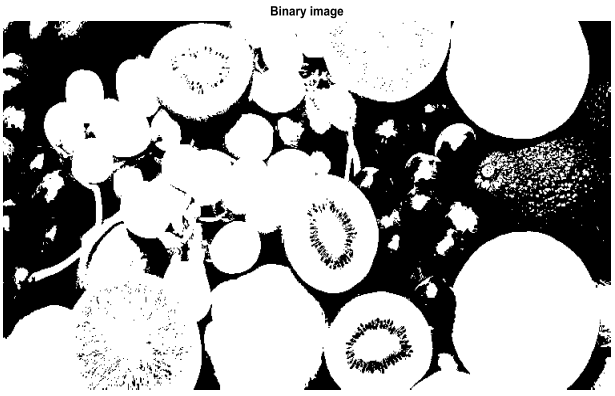

Fig 5

9. Now, this image is encrypted further by using LSB watermarking technique and is hidden further in another image, i.e., Host Image 2 as shown in Fig 6.

Fig 6

10. The image to be hidden, i.e., the encrypted image, after XOR, PN sequencing and RSA ciphering is converted to a binary image and along with the objective image are together shown in Fig 7.

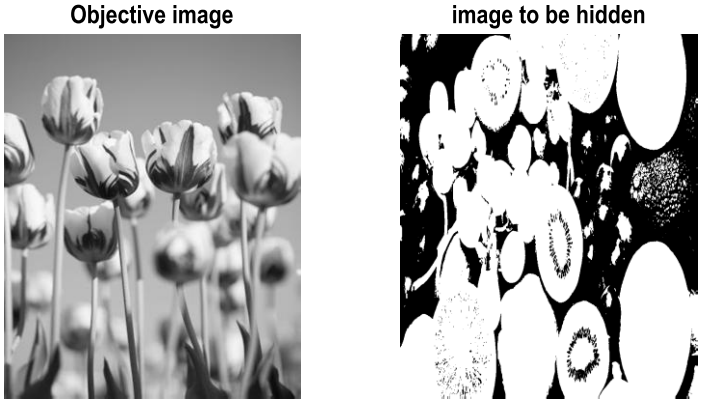

Fig 7

11. The watermarked image after final layer of encryption is shown in Fig 8. LSB technique is used in hiding the data inside the image.


Fig 8

12. Now for all the levels of decryption, all the processes are reverted. The encrypted image is later recovered from the final invisible watermarked image 2 which is shown in Fig 9.

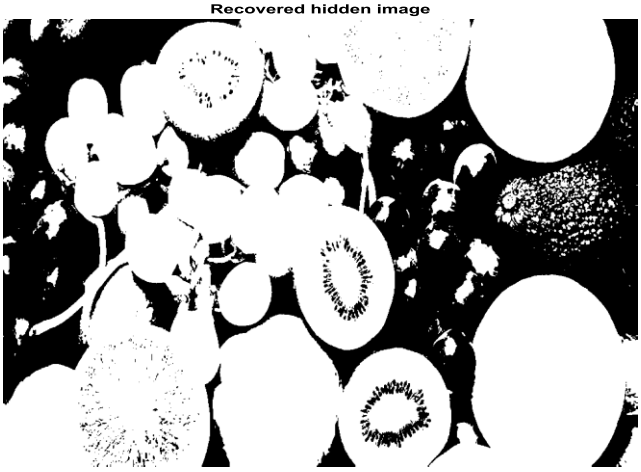


Fig 9

13. Now, Fig 9 contains the encrypted message after the XOR, PN sequencing and RSA algorithm, which are further decrypted:

xor_dec = 'wq$'

pn_dec = 'piH'

14. The concatenated message after the XOR and PN-sequence decryption:

z = 'wq$piH'

15. The decrypted message for the RSA decryption:

m1 = 752 495 545

stn = ' write'

16. At the end, the final concatenated message after the xor and pn-sequence decryption, is decrypted using Fibonacci decryption:

fib_dec = 'Let us'

17. The last message is received by concatenating the two decrypted segments, one from the fibonacci decryption and the other from the RSA decryption. So the original message is now retrieved.
18. Decrypted original text = 'Let us write'

Thus, the original text message is recovered after passing through the various encryption layers of our model.

## IV. CONCLUSION

Data confidentiality has always been an area for research for the past few years. Data encryption makes using the intercepted data by the third party, as difficult as possible, whereas steganography ultimately deals with the hiding of data. Hence these techniques can be applied for data protection. This paper, successfully, develops a scheme for four layered ciphering of the plain text by making the use of Fibonacci series ciphering in a unique way on the segmented data, followed by XOR ciphering and PN sequencing. Also RSA encryption has also been used on one of the segment of the text, further using Steganography for a secure safeguarding. Thus, hybrid data ciphering becomes more secure and hence, the ciphering and watermarking techniques are applied on segmented parts of the plain text which makes if extremely hard even to detect if any information is being exchanged between the two parties. We aim to develop four layers of encryption to safeguard the authenticity of the information to be transferred.

## REFERENCES

1. M. A. Khan, K. K. Mishra, N. Santhi and J. Jayakumari, "A new hybrid technique for data encryption," 2015 Global Conference on Communication Technologies (GCCT), Thuckalay, 2015, pp. 925-929, doi: 10.1109/GCCT.2015.7342801
2. R. Jain and J. Boaddh, "Advances in digital image steganography," 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), Noida, 2016, pp. 163-171. doi: 10.1109/ICICCS.2016.7542298
3. D. Kaur, H. K. Verma and R. K. Singh, "A hybrid approach of image steganography," 2016 International Conference on Computing, Communication and Automation (ICCCA), Noida, 2016, pp. 1069-1073. doi: 10.1109/CCAA.2016.7813901
4. P. Agarwal, N Agarwal, R Saxena, "Data Encryption through Fibonacci Sequence and Unicode Characters," MIT International Journal of Computer Science and Information Technology, Vol. 5, No. 2, August 2015, pp. 79-82 79. ISSN 2230-7621©MIT Publications
5. M. Preetha and M.Nithya, "A study and performance analysis of RSA algorithm," International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 2, Issue. 6, June 2013, pg.126 – 139
6. A. Kaur and S. Singh, "A hybrid technique of cryptography and watermarking for data encryption and decryption," 2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC), Waknaghat, 2016, pp. 351-356, doi: 10.1109/PDGC.2016.7913175.
7. A. Shrivastava and L. Singh, "A new hybrid encryption and steganography technique: a survey," International Journal of Advanced Technology and Engineering Exploration, Vol 3(14) ISSN (Print): 2394-5443 ISSN (Online): 2394-7454 http://dx.doi.org/10.19101/IJATEE.2016.314005.
8. D. Neeta, K. Snehal and D. Jacobs, "Implementation of LSB Steganography and Its Evaluation for Various Bits," 2006 1st International Conference on Digital Information Management, Bangalore, 2007, pp. 173-178. doi: 10.1109/ICDIM.2007.369349.
9. R. Halder, S. Sengupta, S. Ghosh, D. Kundu, "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique," IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 1, Ver. IV (Jan – Feb. 2016), PP 39-43.
10. N. Akhtar, V. Ahamad and H. Javed, "A compressed LSB steganography method," 2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT), Ghaziabad, 2017, pp. 1-7. doi: 10.1109/CIACT.2017.7977371
11. S. Kaur, S. Bansal and R. K. Bansal, "Steganography and classification of image steganography techniques," 2014 International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2014, pp. 870-875.

doi: 10.1109/IndiaCom.2014.6828087
12. M. A. Dagadita, E. I. Slusanschi and R. Dobre, "Data Hiding Using Steganography," 2013 IEEE 12th International Symposium on Parallel and Distributed Computing, Bucharest, 2013, pp. 159-166. doi: 10.1109/ISPDC.2013.29

## AUTHORS PROFILE

**s**

**Shubhankar Saxena is** pursuing Bachelors of Technology in Electronics and Communication Engineering from Vellore Institute of Technology, Vellore, India. His research interests include the fields of cryptography, communication systems, signal processing, image processing, robotics and automation. He has also published a paper based on signal processing in IEEE Explore Digital Library.

**Anushka Sharma is** pursuing Bachelors of Technology in Electronics and Communication Engineering from Vellore Institute of Technology, Vellore, India. Her research interests include the fields of cryptography, communication systems, machine learning, neural networks, deep learning and artificial intelligence.