NSWT : Network security using Walsh Table Algorithms

Syed Jaffar Abbas[1] , Raju Manjhi[2]
Department of Computer Application, Ranchi University , Ranchi , India[1]
Department of Computer Application, Ranchi University , Ranchi , India[2]

Abstract

In this paper we describe a method for integrating Security through Walsh Table . Network Security is becoming more and more crucial as the volume of data being exchanged on the Internet increases. When people use the Internet, they have certain expectations. They expect confidentiality and data integrity. They want to be able to identify the sender of a message. Through this paper we want to send the message to only the intended receiver. To all the other, the message should be unintelligible. We have tried in this paper that the data must arrive at the receiver exactly as it was sent. There must be no changes during the transmission, either accidental or malicious.

Keywords : ***Keyword : Security , Walsh table ,Encryption, NSWT Algorithms.***

1. Introduction

1.1 Security

A *Security* involves four aspects: privacy, message authentication, message integrity, and non-repudiation.

Privacy: It means that the sender and the receiver expect privacy. The transmitted message should make sense to only the intended receiver. To all others, the message should be unintelligible.

Authentication: It means that the receiver is sure of the sender's identity.

Integrity: It means that the data must arrive at the receiver exactly as it was sent. There must be no changes during the transmission, either accidental or malicious. For example, it would be harmful if a request for transferring $200 changes to a request for $20,000. The integrity of the message must be preserved in a secure communication.

Non- Repudiation: It means that a receiver must be able to prove that a receive message came from a specific sender. The sender must not be able to deny sending a message. For example, when a customer sends a message to transfer money from one account to another, the bank must have proof that the customer actually requested this transaction.

Privacy with public key Encryption: In this method, there are two keys : a private key and a public key. The private key is kept by the receiver. The public key is announced to the public.

Imagine system A wants to send a message to user B. System A uses the public key to encrypt the message. When the message is received by B, he uses her private key to decrypt the message. In public key encryption/decryption , the public key that is used to encrypt the algorithm is different from the private key that is used to decrypt the algorithm. The public key is available to the public; the private key is kept by each individual.

Advantages:

1. The whole idea behind public key encryption is to remove the restriction of a shared secret key between two entities who need to communicate with each other.
2. The number of keys needed is reduced tremendously. In this system, for one million user to communicate , only two millions are needed, not a half–billion as was the case in secret key encryption.

1.2Walsh table

We use a Walsh table, which is a two-dimensional table with an equal number of rows and column as shown in below fig.

Two basic rules of Walsh table

$$W_1 = [+1] \qquad (1)$$

$$W_{2N} = \begin{bmatrix} W_N & W_N \\ W_N & \overline{W_N} \end{bmatrix}$$

According to Walsh, if we know the table for N sequences Wn , we can create the table for 2N sequences W_{2N}. the W_N with the over bar stands for the complement of W_N, where each +1 is changed to -1 and vice versa.

1.3 Encryption

The technique for providing confidentiality for transmitted data is symmetric encryption It has four ingredients

Plaintext: This is the original message or data that is fed into the algorithm as input.

Encryption algorithms: The encryption algorithm performs various substitutions and transformations on the plaintext.

Secret key: The secret key is also input to the encryption algorithm. The exact substitutions and transformations performed by the algorithm depend on the key.

Cipher text: This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different cipher texts.

2. Related Work

2.1Methodology: In this paper we develop an algorithm, NS algorithm to encrypt the scanned copy of signature of any customer whose account is in Bank. It must be secure that nobody can change data during the transmission, either accidental or malicious. The process to do this work is following;
Step 1: First scan the copy of signature of any customer.
Step 2: Convert the scan signature files into the binary picture file,binarypicture.jpg .
Step 3: Convert binarypicture.jpg into the binary text file.
Step 4: Fit this converted binary text file into NXN matrix.
Step 5: Multiply **NXN** matrix with Walsh table denoted by Wn.
Step 6: Resultant matrix will be the encrypted data that nobody can see it.

a).Two basic rules of Walsh table

(1) $W_1 = [+1]$

(2) $W_{2N} = \begin{bmatrix} W_N & W_N \\ W_N & \overline{W_N} \end{bmatrix}$

b).Let n = 0,1 , 2 , 3 ,……………… r
then N= power of (2^n)
Generation of W2,W4,W8,W16,W32…………

$$W_2 = \begin{bmatrix} W_1 & W_1 \\ W_1 & \overline{W_1} \end{bmatrix}$$

$$= \begin{bmatrix} +1 & +1 \\ +1 & -1 \end{bmatrix}$$ **Byapplying rule (1)**

Equation (2)

Replace +1 by $\begin{bmatrix} +1 & +1 \\ +1 & -1 \end{bmatrix}$

And -1 by $\begin{bmatrix} -1 & -1 \\ -1 & +1 \end{bmatrix}$

Equation (3)

From equation (2) and (3)

$$W_4 = \begin{bmatrix} +1 & +1 & +1 & +1 \\ +1 & -1 & +1 & -1 \\ +1 & +1 & -1 & -1 \\ +1 & -1 & -1 & +1 \end{bmatrix}$$

Equation (4)

From equation (3) and (4)

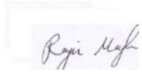
$$W_8 = \begin{bmatrix} +1 & +1 & +1 & +1 & +1 & +1 & +1 & +1 \\ +1 & -1 & +1 & -1 & +1 & -1 & +1 & -1 \\ +1 & +1 & -1 & -1 & +1 & +1 & -1 & -1 \\ +1 & -1 & -1 & +1 & +1 & -1 & -1 & +1 \\ +1 & +1 & +1 & +1 & -1 & -1 & -1 & -1 \\ +1 & -1 & +1 & -1 & -1 & +1 & -1 & +1 \\ +1 & +1 & -1 & -1 & -1 & -1 & +1 & +1 \\ +1 & -1 & -1 & +1 & -1 & +1 & +1 & -1 \end{bmatrix}$$

Equation (5)

From equation (3) and (5)

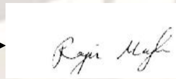
$$W_{16} = \begin{bmatrix} +1 & +1 & +1 & +1 & +1 & +1 & +1 & +1 & +1 & +1 & +1 & +1 & +1 & +1 & +1 & +1 \\ +1 & -1 & +1 & -1 & +1 & -1 & +1 & -1 & +1 & -1 & +1 & -1 & +1 & -1 & +1 & -1 \\ +1 & +1 & -1 & -1 & +1 & +1 & -1 & -1 & +1 & +1 & -1 & -1 & +1 & +1 & -1 & -1 \\ +1 & -1 & -1 & +1 & +1 & -1 & -1 & +1 & +1 & -1 & -1 & +1 & +1 & -1 & -1 & +1 \\ +1 & +1 & +1 & +1 & -1 & -1 & -1 & -1 & +1 & +1 & +1 & +1 & -1 & -1 & -1 & -1 \\ +1 & -1 & +1 & -1 & -1 & +1 & -1 & +1 & +1 & -1 & +1 & -1 & -1 & +1 & -1 & +1 \\ +1 & +1 & -1 & -1 & -1 & -1 & +1 & +1 & +1 & +1 & -1 & -1 & -1 & -1 & +1 & +1 \\ +1 & -1 & -1 & +1 & -1 & +1 & +1 & -1 & +1 & -1 & -1 & +1 & -1 & +1 & +1 & -1 \\ +1 & +1 & +1 & +1 & +1 & +1 & +1 & +1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ +1 & -1 & +1 & -1 & +1 & -1 & +1 & -1 & -1 & +1 & -1 & +1 & -1 & +1 & -1 & +1 \\ +1 & +1 & -1 & -1 & +1 & +1 & -1 & -1 & -1 & -1 & +1 & +1 & -1 & -1 & +1 & +1 \\ +1 & -1 & -1 & +1 & +1 & -1 & -1 & +1 & -1 & +1 & +1 & -1 & -1 & +1 & +1 & -1 \\ +1 & +1 & +1 & +1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & +1 & +1 & +1 & +1 \\ +1 & -1 & +1 & -1 & -1 & +1 & -1 & +1 & -1 & +1 & -1 & +1 & +1 & -1 & +1 & -1 \\ +1 & +1 & -1 & -1 & -1 & -1 & +1 & +1 & -1 & -1 & +1 & +1 & +1 & +1 & -1 & -1 \\ +1 & -1 & -1 & +1 & -1 & +1 & +1 & -1 & -1 & +1 & +1 & -1 & +1 & -1 & -1 & +1 \end{bmatrix}$$

Similarly we can generate W_{32} and so on



Scan Signature

Stage 1 : Process for converting Scan Signature into Binary value



Binarypicture.jpg

111111111111111
111000000000001
111111111111100

Converted Binary Value

Stage 2 : Process for Encryption

1111111
1111111
1110000
0000001
1111111
1111100
0001111
1100…

→ $[n \times n]$ *matrix* x $[\mathbf{W_{2N}}]$ →

Encrypted data

Converted Binary value

Converted Binary stored n x n matrix

Walsh table

2.2 The Proposed NSWT Algorith

The Proposed NSWT algorithm is used to secure the signature of the customer of any Bank.
In this algorithm, firstly we take the scan signature of the customer and then convert this scan signature into the binary picture.jpg. Secondly, we are converting the binary picture into the binary value and storing that binary value into the Matrix, multiplying it with the Walsh table, the resultant matrix will be encrypted data.

Algorithm NSWT (sign,R)

Input: A Scan signature image denoted by sign and random number ,R.

Output: A set of Encrypted data denoted by enc.

1. Put the scan signature image (thumb.jpg) .
2. for x<-0 to sign.getWidth()
3. for y<-0 to sign.getHeight()
4. do Color picture <- Color(sign.getRGB(x, y));
5. r <- picture.getRed();
6. g <- picture.getGreen();
7. b <- picture.getBlue();
8. Average <- (r+g+b)/3;
9. if average<140
10. the Color new_pixel<- Color(0,0,0);
11. thumb.setRGB(x, y,new_pixel.getRGB());
12. Source<- source.concat("0");
13. else
14. Colornew_pixel<- Color(255,255,255);
15. sign.setRGB(x, y,new_pixel.getRGB());
16. source=source.concat("1");
17. ImageIO.write(thumb, "jpg", newFile("Binary_signature.jpg");
18. bytebinary[<- source.getBytes(); Now the new file will be converted into binary picture and then converted into binary file in text format.
19. Select a random number R <- 0 to n
20. Store the converted binary value.
21. data <- binary[]
22. x <- power of (2^R)
23. tn[][]<- int[x][x];
24. Wn[0][0] <- 1;
25. for i<-0to x.
26. for j<-0to x
27. Count <- count+1.
28. cnt <- count-1.
29. c=data.charAt(cnt).
30. k <- c;
31. tn[i][j]=k;
32. tn[i][j]=0;
33. for l <-1to lessthan x.
34. for i <-0 to less than l.
35. for j <-0 to less than l.
36. do
    wn[i+l][j] <- wn[i][j].
    wn[i][j+l] <-wn[i][j].
    wn[i+l][j+l] <- wn[i][j]*(-1).
37. for i <-0 to less than x.
38. for j <-0 to less than x.
39. for k <-0 to less than x.
40. do
    cn[i][j] <- cn[i][j]+tn[i][k]*wn[k][j];
41. for i<-0 to less than l.
42. for j<-0 to less than l.
43. enc <- cn[i][j]); // Encrypted data
44. return enc.

3. CONCLUSION

Through this paper we have tried to develop an algorithm to stop fraud and duplicate signature of the customer can be checked for in this system. Hence if this system is employed data must arrive at the receiver exactly as it was sent. Thanks to this system that secures the signature of the customer that nobody can change data during the transmission, either accidental or malicious.

References

[1] Albert Bodo, "Method for producing a digital signature with aid of a biometric feature", German patent DE 42 43 908 A1, (1994).
[2] J. Daugman, "High confidence visual recognition of persons by a test of statistical independence", *IEEE Trans. on Pattern Analysis and Machine Intelligence* **15**, 1148-1161, (1993)
[3] J.W. Goodman, *Introduction to Fourier Optics*, McGraw-Hill, (1968).
[4] S.T. Walker, " Network Security: The parts of the sum", proc. 1989 IEEE symp; on Research in security and privacy, Oakland, CA, PP. 2-8, May 1989.
[5] V. Voydock and S.kent, " Security in high-level network protocols, " IEEE communication magazine, PP. 12-24,july 1985.
[6] Bruce Schneier, *Applied Cryptography, 2nd Ed.*, John Wiley & Sons, Inc., New York, (1996).
[7] Federal Information Processing Standards Publications (FIPS 197), "Advanced Encryption Standard (AES) ", 26 Nov. 2001.
[8] K. Gaj, P.Chodowiec, "Fast implementation and fair comparison of thefinal candidates for advanced encryption standard using field programmable gate arrays", in : *CT-RSA 2001*, pp.84-99.
[9] Data Communication and Networking BY Behrouz A Forouzan
[10] T.Aura. Internet-Draft: Cryptographically Generated Addresses (CGA), Microsoft Research, February 2004
[11] W. Diffie and M.E. Hellman. Special feature Exhaustive Cryptanalysis of the NBS Data Encryption Standard Computer, 10(6):74, june 1977