A Secured Wireless Crypto System For Text And File Using Dwt And Blowfish Algorithm

B.Arun[1], K.Shanmuga priya[2]

[1]*Faculty of EEE Department in RVS College of Engineering, Dindigul, Tamilnadu, India (Anna University, Chennai)*

[2]*Student of Master of Engineering in Embedded System Technologies, RVS College of Engineering, Dindigul,Tamilnadu,India (Anna University, Chennai)*

ABSTRACT

Some of the important parameters of the blowfish encryption algorithm are being analyzed and examined to see how these parameters may affect the performance of the algorithm. The performance indices here are the security and speed of the algorithm. This study is applied to different types of data; text, sound and image. For each case the encryption/decryption key length has been changed and its effect on the performance was noticed. Moreover, the file size is changed and its affect on the performance of the algorithm was noticed. This has shown that changing the key length has no effect on the encryption or decryption time whereas changing the plaintext file size is directly reflected on the processing time. The results obtained here have been converted into modules of equations of high orders thus the future performance of the algorithm may be predicted from these equations. Blowfish algorithm (BA) is a symmetric block cipher with a 64-bit block size and variable key lengths from 32 bits up to a maximum of 448 bits. In order to measure the degree of security of blowfish algorithm, some cryptographic tests must be applied such as randomness test, avalanche criteria and correlation coefficient. And it is modified as well as comprised by dwt method, this method is working under the principle of minimized data comprising. The encrypted file was send by a wireless network. The coding return in the visual basic because it is a visual and real time implemented module. However the communication is bidirectional, so dual way communication is possible.

Keywords: *DWT, BLOWFISH,AES, DES.*

1. INTRODUCTION

In the world of internet communication, security plays an important role and owns a major regime on its stack. Now a day’s data security and data integrity are challenging areas. Thus security is the key to unlock a communication box. Branch of security, which are cryptography, information hiding etc, provides better role as they take part. As the technology keeps on changing its face with advanced features, there is necessary to get update. Data security means protection of data from unauthorized users and hackers. So it is necessary to develop algorithms more efficient and unbreakable. The network security is branched into cryptography and information hiding. In cryptography, encryption of data’s takes place at the transmitter and decryption at the receiver section. Thus to encrypt and decrypt same key or different keys may be used. Now extending its branches into symmetric (conventional) and asymmetric (public key) encryption.

Cryptography is a method of storing and transmitting data in a form that only those, it is intended for can read and process. It is a science of protecting information by encoding it into an unreadable format. It is an effective way of protecting sensitive information as it is stored on media or transmitted through network communication paths. To encrypt the data various cryptographic algorithms such DES, 3DES, blowfish, AES, etc are used. So we are implementing blowfish algorithm which is strongest and fastest in data processing/storing compare to other algorithms which is mentioned above. Blowfish algorithm is highly secured because it has longer key length (more no of key size).

2. LITERATURE REVIEW

2.1 Performance Evaluation of DES and Blowfish Algorithms.

Tingyuan Nie, Chuanwang Song and Xulong Zhi.

Encryption algorithm plays an important role for information security guarantee. In this paper, we evaluate the performance of two symmetric key encryption algorithms: DES and Blowfish which commonly used for network data encryption. In this paper, we analyzed encryption security, evaluated encryption speed and power consumption for both algorithms. Experimental results show that Blowfish algorithm runs faster than DES, while the power consumption is almost the same. It is proved that the Blowfish encryption algorithm maybe more suitable for wireless network application security.

2.2 Research and Implementation of RSA Algorithm for Encryption and Decryption

Xin Zhou and Xiaofei Tang.

Encryption and decryption algorithm's security depends on the algorithm while the internal structure of the rigor of mathematics, it also depends on the key confidentiality. Key in the encryption algorithm has a pivotal position, once the key was leaked, it means that anyone can be in the encryption system to encrypt and decrypt information, it means the encryption algorithm is useless. Therefore, what kind of data you choose to be a key, how to distribute the private key, and how to save both data transmission keys are very important issues in the encryption and decryption algorithm.

3. PROPOSED SYSTEM

To develop a cryptosystem for image and audio using DWT and Blowfish algorithm. Blowfish is a Feistel network consisting of 16 rounds symmetric block encryption algorithm.

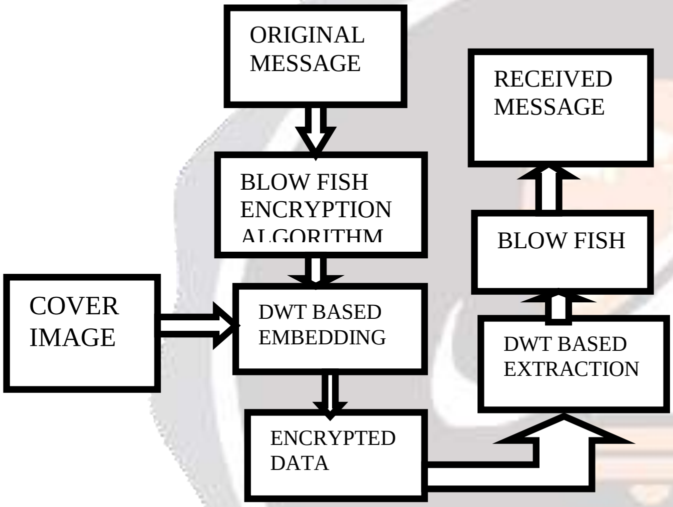


Figure 1 Block Diagram of Proposed system

DWT is an another method used in our system which is used to split the data into small wavelets and the bandwidth of the image is compressed for the secured transmission. Before hiding, the image is transformed from spatial domain to frequency domain using DWT (Discrete Wavelet Transform) algorithm. DWT divides the image into sub bands in which we hide out text. Text is hidden using least significant bit algorithm in frequency domain. The image is obtained which is sent to receiver. Message is extracted and decrypted to get original message.

Sender side:

1. Write text message.(original message).
2. Encrypt message using Blowfish algorithm.
3. Select cover image.
4. Use DWT algorithm for transforming the image and then hide the message into image to get the image.

Receiver side:

1. Receive the image.
2. Use DWT algorithm to extract message from image.
3. Decrypt message using Blowfish algorithm.
4. Get original message.

4. BLOWFISH ALGORTHIM

Blowfish is a symmetric block cipher that can be effectively used for encryption and safeguarding of data. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. Blowfish was designed in 1993 by **BrucSchneier** as a fast, free alternative to existing encryption algorithms.

Fast: It encrypts data on large 32-bit microprocessors at a rate of 26clock cycles per byte.

Compact: It can run in less than 5K of memory.
Simple: It uses addition, XOR, lookup table with 32-bit operands.
Secure: The key length is variable ,it can be in the range of 32~448 bits: default 128 bits key length.

4.1 Description Of The Algorithm

Blowfish is a variable-length key, 64-bit block cipher. The algorithm consists of two parts a key-expansion part and a data- encryption part. Key expansion converts a key of at most 448 bits into several sub key arrays totaling 4168 bytes. Data encryption occurs via a 16-round Feistel network. Each round consists of a key dependent
permutation, and a key- and data-dependent substitution.

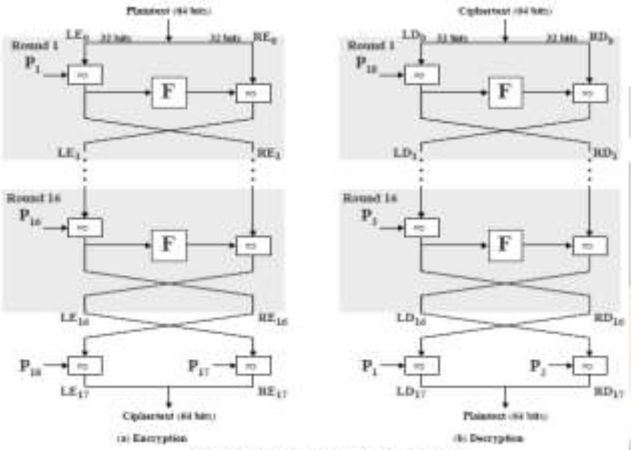


Figure 2 Block Diagram of BLOWFISH Algorithm

All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round.

Subkeys

Blowfish uses a large number of subkeys. These keys must be pre computed before any data encryption or decryption.

- The P-array consists of 18 32-bit subkeys:P1, P2,..., P18.
- There are four 32-bit S-boxes with 256 entries each:

S1,0, S1,1,..., S1,255;
S2,0, S2,1,..,, S2,255;
S3,0, S3,1,..., S3,255;
S4,0, S4,1,..,, S4,255.

Encryption

Blowfish has 16 rounds.
The input is a 64-bit data element, x.
Divide x into two 32-bit halves: xL, xR.
Then, for i = 1 to 16:
xL = xL XOR Pi
xR = F(xL) XOR xR
Swap xL and xR
After the sixteenth round, swap xL and xR again to undo the last swap.
Then, xR = xR XOR P17 and xL = xL XOR P18.
Finally, recombine xL and xR to get the ciphertext.
Decryption is exactly the same as encryption, except that P1, P2,..., P18 are used in the reverse order.
Implementations of Blowfish that require the fastest speeds should unroll the loop and ensure that all subkeys are stored in cache.

5. DISCRETE WAVELET TRANSFORM (DWT)

The DWT represents an image as a sum of wavelet functions, known as wavelets, with different location and scale. It represents the data into a set of high pass (detail) and low pass (approximate) coefficients. The input data is passed through set of low pass and high pass filters. The output of high pass and low pass filters are down sampled by 2.The output from low pass filter is an approximate coefficient and the output from the high pass filter is a detail coefficient.

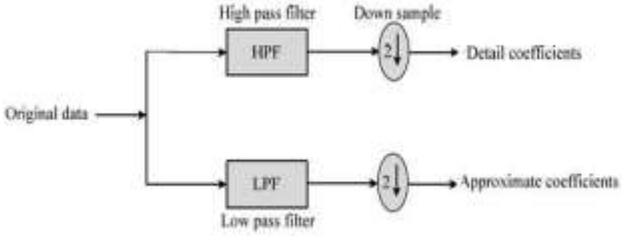


Figure 3 Block Diagram Of 1-D Foward DWT

In case of 2-D DWT, the input data is passed through set of both low pass and high pass filter in two directions, both rows and columns. The outputs are then down sampled by 2 in each direction as in case of 1- D DWT. As output is obtained in set of four coefficients LL, HL, LH and HH.

The first alphabet represents the transform in row where as the second alphabet represents transform in column. The alphabet L means low pass signal and H means high pass signal. LH signal is a low pass signal in row and a high pass in column. Hence, LH signal contain horizontal elements. Similarly, HL and HH contains vertical and diagonal elements, respectively.

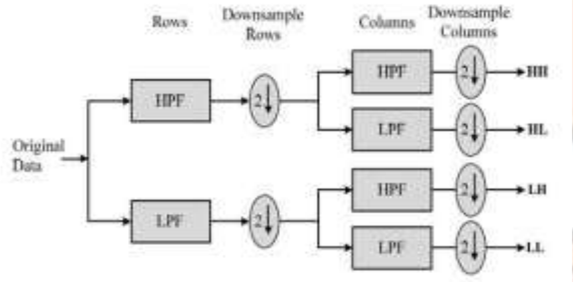


Figure 5 Block Diagram Of 2-D Forward

6. OUTPUT SCREEN

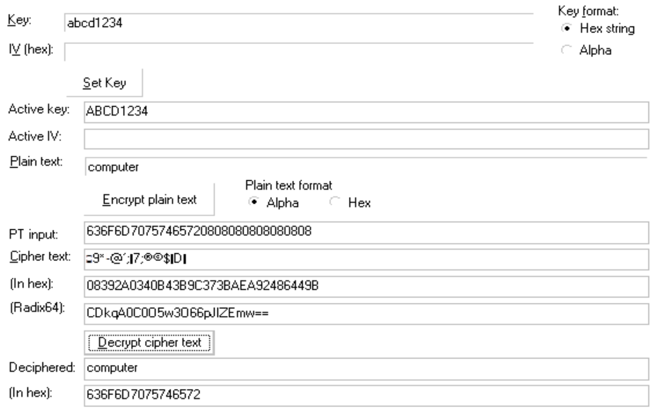
6.1 Visual Studio Screen

By using Dot Net software we can send the string (text)and file(bunch of data or folder,audio,video,image,etc) in this software by using Blowfish algorthim,RC2,RSA,DES,AES,etc.

By using .NET we can see the function and we send the message easily, it take too less time to send the message. by choosing the algorithm we see the difference of key format. Now a Day it is the more secure way to transfer the data to other end.

BLOWFISH AND DWT RESPONSE

In this screen enter the key(password),and texted data,audio,video,etc. and choose the algorithm type and then set the key format by using DWT ,DWT is the background processor ,the function of DWT is compress the data or image in 1-D or 2-D forward matrix by using alpha or hex.


Key: abcd1234

IV (hex):

Key format: ● Hex string ○ Alpha

Active key: ABCD1234

Active IV:

Plain text: computer

Plain text format ● Alpha ○ Hex

PT input: 636F6D70757465720808080808080808

Cipher text: ⌐9ª-@´;‖7;®©$‖D‖

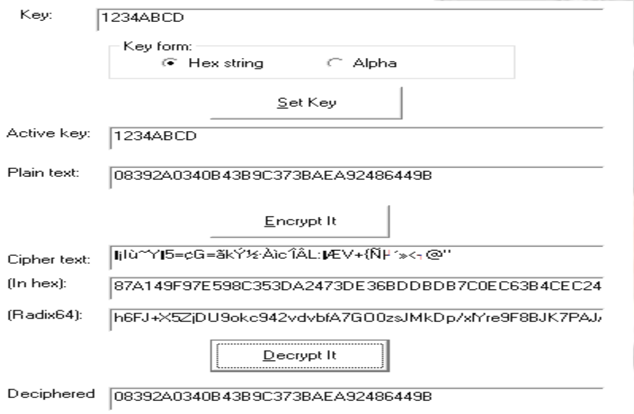
(In hex): 08392A0340B43B9C373BAEA92486449B

(Radix64): CDkqA0C0O5w3O66pJIZEmw==

Deciphered: computer

(In hex): 636F6D7075746572

Figure 6 Blowfish Response (visual studio screen)


Key: 1234ABCD

Key form: ● Hex string ○ Alpha

Active key: 1234ABCD

Plain text: 08392A0340B43B9C373BAEA92486449B

Cipher text: ‖¡Iù~Y‖5=¢G=ãkÝ½·Àic΄ÎÂL:‖ÆV+{Ñ⊦´»<¬@"

(In hex): 87A149F97E598C353DA2473DE36BDDBDB7C0EC63B4CEC24

(Radix64): h6FJ+X5ZjDU9okc942vdvbfA7GO0zsJMkDp/xfYre9F8BJK7PAJ

Deciphered 08392A0340B43B9C373BAEA92486449B

Figure 7 DWT Response (visual studio screen)

Applications

- Secure medical and military image data system
- Law enforcement
- E-government
- Image authentication
- Covert Communication

CONCLUSION

In cryptography the message being sent at one end remains confidential and should be received only by the intended receiver at the other end(for simplify to reduce the panel we design in single panel). Even though many cryptographic algorithms are developed. We compare some algorithm on the basis of certain parameters. Some of algorithm are flexible some of them provides high security and some of them are modifiable. By Surveying many papers, I have found that throughput value of BLOWFISH is greater than all symmetric algorithms. Power Consumption value of BLOWFISH is least. It has better performance and efficiency than all other block ciphers.

ACKNOWLEDGMENT

This project is funded for Master of Engineering in Embedded System Technologies under the Anna University, Chennai, In the academic year 2016-2017.

REFERENCES

1. Pramod Gorakh Patil, Vijay Kumar Verma “A Recent Survey on Different Symmetric Key Based Cryptographic Algorithms”, IJCAT - International Journal of Computing and Technology, Volume 3, Issue 2, February 2016.

2. Sanket A. Ubhad, Prof. Nilesh Chaubey, Prof. Shyam P.DubeyASCII Based “Cryptography Using Matrix Operation, Palindrome Range”,Uniqueid International Journal of Computer Science and Mobile Computing IJCSMC, Vol. 4, Issue. 8, August 2015.

3. Saranya K and Mohanapriya R “A Review on Symmetric Key Encryption Techniques in Cryptography”.International Journal of Science, Engineering and Technology Research (IJSETR), Volume 3, Issue 3, March 2014.

4. B.Geethavani, E.V.Prasad and R.Roopa 2013, "A Modified Approach for Symmetric Key Cryptography Based on Blowfish Algorithm", International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization).

5. Monika Agrawal, Pradeep Mishra “Modified Approach for Symmetric Key Cryptography Based on Blowfish Algorithm” International Journal of Engineering and Advanced Technology (IJEAT)ISSN: 2249 – 8958, Volume-1, Issue-6, August 2012.