International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Cryptography in Image Using Blowfish Algorithm

S. S. Sudha[1], S. Divya[2]

[1]Assistant Professor, Dept of CS, PSG College of Arts & Science, Coimbatore, Tamilnadu, India

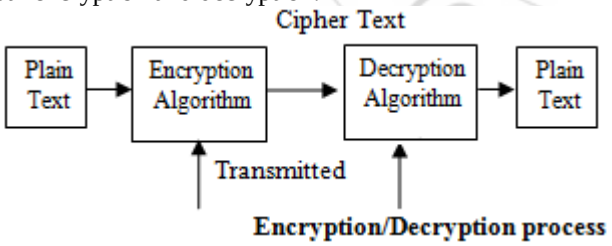
[2]Research scholar, Dept of CS, PSG College of Arts & Science, Coimbatore, Tamilnadu, India

Abstract: ***Cryptography is the art of secrete writing; cryptography is the science of encrypting the image. The study of encrypting is converting the original information from its normal form to incomprehensible format. These days securing the data's has become difficult, to reduce the complexity, cryptography has been used. Image data security is the indispensable portion in communication, defence and networks and so many. Providing security is more important for the image. In this paper securing the image is executed with a "Blowfish algorithm" from the perspective of cryptology. Blowfish is used for the applications, where the key doesn't change often and has a larger space to store the data. Encryption and decryption is performed to obtain the original hiding information from the image.***

Keywords: Cryptography, Encryption, Decryption, Secrete key, Blowfish Algorithm

1. Introduction to Cryptography

Cryptography in practise is recognized as a message in its plaintext or clear text. The mangled information is known as cipher text. The process for creating cipher text from plaintext is known as encryption. The transitive process of encryption is called decryption. Many sectors like government, industries, IT industries, hospitals, defence, space centres deals with confidential messages and images. Information is collected and stored on computers and transmitted across network to other computer. Before transmitting the data has to be secured for that the data's has to be encrypt or encode, this prevents from hacking the data or the information. Cryptography is tend to comprise both algorithm and a secrete value. Blowfish algorithm is highly protected because of the fixed 64 bit block size. Key length of Blowfish can be anywhere from 32 bits to 448 bits. It has longer key length (more no of key size). In this the secrete value is known as the key. There are two types key one is private key and another one is public key. Key is used for both encryption and decryption.

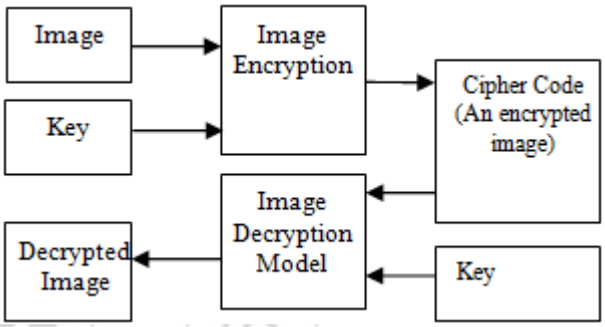


Encryption/Decryption process

Cryptography

The word cryptography comes from the Greek words, crypto refers to hidden or secrete and graph refers to writing. Cryptography is the art of writing the secret messages with the image or in any form. Hiding the original information with the different format manages the security of the images. The main work of the cryptography is to send the messages between receiver and the sender, in a way that prevents other participants from reading the messages.

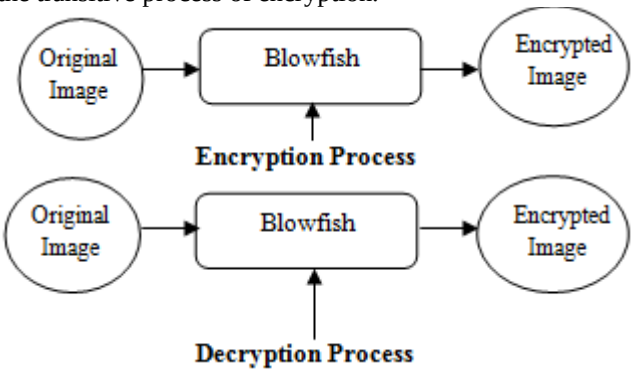
The mangled information is known as cipher text. The process for producing cipher text from plaintext is known as encryption. The transitive process of encryption is called decryption. Cryptosystem two processes are applied, converting of the original image data in to some other unidentified structure using a key. In this paper private key is used to lock and unlock the messages, by which the single key the messages can be encrypt and decrypt and recover the plain text.



Architecture of Cryptography

2. Encryption and Decryption

When someone wants to send a message to a receiver and wants that message to be confidential, such that no other persons can read the text or the message. There is a possibility of hacking the messages that send through internet and also by other means. To avoid this, encryption and decryption is applied so that the message will secure. Means that the third party can't be hack or read the message. It is impossible to read the message without the appropriate knowledge. This is processed by encryption. Decryption is the transitive process of encryption.



2.1 Secrete Key cryptography

In Secrete Key Cryptography (SKC), single key is used for both encryption and decryption. When A sends a message, uses the key to encrypt the plain text and sends the cipher text to B. B uses the same key to decrypt the image and gets the original plain text. Secrete key is also known as asymmetric key. Same key is generated for the encryption and decryption. The message that received to B can decrypt the message using the private key, the private key is only known to the sender and the receiver (i.e) A and B. The sender generates the private key.

3. Blowfish Algorithm

Blowfish was designed in 1993 by Bruce Schneier, it became as a fast and free alternative to existing encryption algorithms. Blowfish algorithm is much faster than the DES algorithm; it is designed in a way to fulfil all the aspects.

Speed:
Blowfish algorithm is faster than the DES algorithm with the block size of 64 bitsand the key can be any length up to 448bits.

Compactness:
It can run in a small memory space, less than 5K.

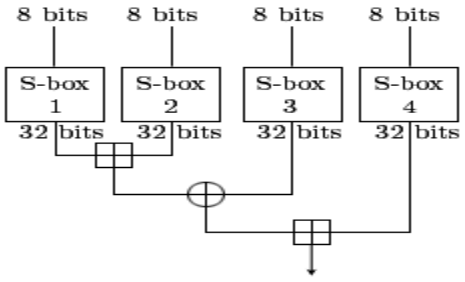
Simplicity:
Simple operations are used, including addition, exclusive-or, and table lookups.

Flexibility of key size:
The key doesn't change often.

Blowfish algorithm encrypts block data of 64-bits at a time; it will follow the Feistel network. There are the P-arrays and the S-boxes, which P- arrays have eighteen 32-bit boxes, and the S- boxes are four 32-bit arrays with 256 entries each. All operations are XORs and additions on 32-bit words. Four indexed array data lookups per round are the additional operator.

3.1 Key generation

• Large number of sub keys is used in blowfish.
• The p-array consists of 18, 32-bit sub keys
P1,P2,……,P18
• S-Boxes consist of 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

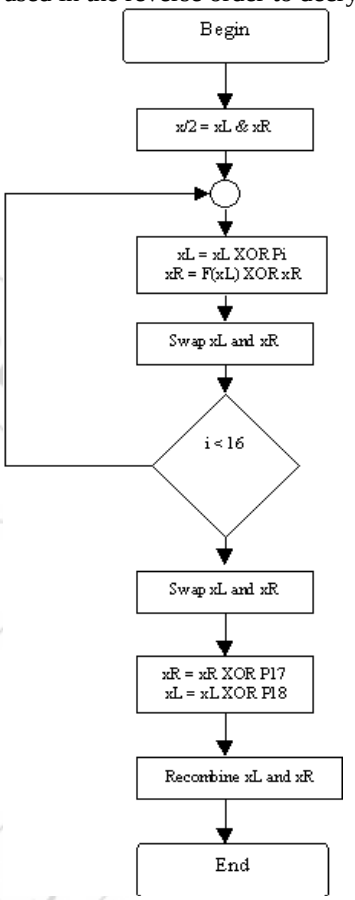


The Feistel Function of Blowfish

Encryption and Decryption: There are16 rounds in blowfish; input is a 64-bit data element, x. x is divided into two 32-bit halves: xL, xR[8]. Then, for i = 1 to 16

Xl = xL XOR Pi
xR = F(xL) XOR xR
And Swap xL and xR

After the sixteenth round, xL and xR are has to swap again to undo the last swap. Then, xR = xR XOR P17 and xL = xL XOR P18. Recombine xL and xR to get the cipher text.P1, P2,..., P18 are used in the reverse order to decrypt.



Block Diagram of Data Encryption

3.2 Steps to Generate Sub Keys

1) Initialize first the P-array and then the four S-boxes.
2) The first 32 bits of the key is with XOR P1, the second 32-bits of the key is with XOR P2.
3) Encrypt the all-zero string with the Blowfish algorithm, using the sub keys described in steps (1) and (2).
4) This new output is now P1 and P2.
5) Encrypt the output of step (3) using the Blowfish algorithm with the modified sub keys.
6) This new output is now P3 and P4.
7) Repeat 521 times in order to calculate the new sub keys for the P- array and Four S- boxes.

4. Conclusion and Future Scope

In this paper to transmit encrypting image over the internet we have used the blowfish algorithm. Previously used algorithm like AES, DES and so more has been replaced by the blowfish algorithm, because of producing successful

effectiveness on security. Blowfish algorithm can't be easily broken by the hackers until they find the correct combinations. This is more difficult to form the exact combinations of the lock. To make the algorithm stronger number of rounds has been increased. It takes less time to encrypt and decrypt the image than any other algorithms. For future enhancement advanced algorithms can be invent for better security and helps to encrypt more complicated image.

References

[1] Anjaneyulu GSGN, Pawan Kumar Kurmi, Rahul Jain, Image Encryption And Decryption Using Blowfish Algorithm With Random Number Generator, Anjaneyulu GSGN* et al. International Journal Of Pharmacy & TechnologyIJPT| Jan-ISSN: 0975-766X
[2] Mrs.Smita Desai1, Chetan A. Mudholkar, RohanKhade, PrashantChilwant Image Encryption And decryption Using Blowfish Algorithm, IJEEE, Volume 07, Issue 01, Jan- June 2015 International Journal of Electrical and Electronics Engineers ISSN-2321-2055 (E)
[3] Tanjyot Aurora, ParulArora, Blowfish Algorithm, "Recent Advances in Engineering & Technology" International Journal of Computer Science and Communication Engineering, IJCSCE NCRAET-2013, ISSN 2319-7080
[4] JyotikaKapur, Akshay. J. Baregar, Security Using Image Processing, International Journal of Managing Information Technology (IJMIT) Vol.5, No.2, May 2013
[5] Sujay Narayana1and Gaurav Prasad2, two New Approaches For Secured Image Steganography Using Cryptographic Techniques And Type Conversions, Signal & Image Processing : An International Journal(SIPIJ) Vol.1, No.2, December 2010
[6] HiralRathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma, Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm (Hyper Image Encryption Algorithm), International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 1, Issue 3
[7] KundankumarRameshwarSaraf, Vishal PrakashJagtap, Amit Kumar Mishra, Text and Image Encryption Decryption Using Advanced Encryption Standard,International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
[8] S.Dhanalakshmi, Dr.T.Ravichandran, A New Level Of Image Processing Technique Using Cryptography And Steganography, ISSN: 2278 – 7798 International Journal of Science, Engineering and Technology Research (IJSETR) Volume 2, Issue 3, March 2013 659
[9] Kaladharan N, Unique Key Using Encryption and Decryption of Image, International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 10, October 2014
[10] Mayank Mishra, Prashant Singh, ChinmayGarg, A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping, International Journal of Information & Computation Technology. ISSN 0974-2239 Volume 4, Number 7 (2014), pp. 741-746

Author Profile

S. S. Sudha , Assistant Professor, Dept of CS, PSG college of Arts & Science, Coimbatore, Tamilnadu

S. Divya, Research scholar, Dept of CS, PSG college of Arts & Science, Coimbatore, Tamilnadu.