International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Blowfish Algorithm by Modify Randomness for S-Boxes using Fuzzy Value and Apply Encryption or Decryption on Image

Maulik P. Chaudhari[1], Neha Parmar[2]

[1]Computer Science & Engg., Parul Institute of Technology, P.O.Limda, Ta.Waghodia - 391760
Dist. Vadodara, Gujarat (India),

[2]Assistant Professor, Computer Science & Engg., Parul Institute of Technology, P.O.Limda, Ta.Waghodia - 391760
Dist. Vadodara, Gujarat (India),

Abstract: ***Information Security has been most important issue in data communication. Any loss or threat to information can prove to be big loss to the organization. Encryption technique plays an important role in information security systems. Information security area there are many cryptography algorithm is available and comparison has been made on the basis on these parameters: rounds block size, key size, and encryption / decryption time, CPU process time in the form of throughput and power consumption. These results show that blowfish is better than other algorithm. Blowfish is more secure and fast computing algorithm. But there is some problem in the existing Blowfish algorithm .blowfish weak keys generates "bad" S-boxes, Since Blowfish's S-boxes are key dependent. There is a chosen plaintext attack against a reduced-round variant of blowfish algorithm that is made easier by the use of weak key. in this report proposed a new approach to increase the robust of blowfish algorithm and solve the weakness of sub key by generate strongest a cryptographic randomness keys and used in blowfish's S- boxes stages. The proposed algorithm the secret key changes frequently by using randomness fuzzy value which are derived by different fuzzy set of condition after modify algorithm apply encryption and decryption on image and also Modified the F function operation to use of Multithreading to improve the Execution time and improve the Security by the new key generation approach.***

Keywords: Cryptography, Blowfish Algorithm, Fuzzy Logic, Fuzzification, Defuzzification.

1. Introduction

The U.S National Information System Security Glossary defines "Information Systems Security" as the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats [14]. 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 [18].

1.1. Cryptography

Cryptography is the science that studies the mathematical techniques for keeping message secure and free from attacks [4].
We define some terms. An original message is known as the plaintext, while the coded message is called the ciphertext.The process of converting from plaintext to cipher text is known as enciphering or encryption; restoring the plaintext from the cipher text is deciphering or decryption. The many schemes used for encryption constitute the area of study known as cryptography. Such a scheme is known as a cryptographic system or a cipher. Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of cryptanalysis. Cryptanalysis is what the layperson calls "breaking the code. "The areas of cryptography and cryptanalysis together are called cryptology [18].

Information security remains a challenge. As such, ciphers appropriate for the security of specific applications need to be developed. Algorithms and performance security of a given algorithm is dependent on various parameters including size of key and block, diffusion, and confusion properties [16].

The current cipher design is still guided by the principles of confusion and diffusion. Confusion is designed to hide the relationship between the plaintext and cipher text. This will discourage the attacker who attempts to locate the key using cipher text. On the other hand, diffusion is supposed to disseminate the plaintext statistics through the cipher text in order to discourage the attacker attempting to locate the plaintext using the cipher text statistics [16].

1.2 Goals of Cryptography

Cryptography provides a number of security goals to ensure the privacy of data, non-alteration of data and so on. Due to the great security advantages of cryptography it is widely used today [7].
Following are the various goals of cryptography.

- Confidentiality
  Information in computer is transmitted and has to be accessed only by the authorized party.
- Authentication

Licensed Under Creative Commons Attribution CC BY

The information received by any system has to check the identity of the sender that whether the information is arriving from a authorized person or a false identity.

- Integrity
  Only the authorized party is allowed to modify the transmitted information. No one in between the sender and receiver are allowed to alter the given message.
- Non Repudiation
  Ensures neither the sender, nor the receiver of message can deny the transmission.
- Access Control
  Only the authorized parties are able to access the given information.

1.3 Type of Cryptography

Cryptography system can be classified into two parts:
1) Symmetric – key Cryptography and
2) Asymmetric – key cryptography.

1. Symmetric – key cryptography:
In symmetric key cryptography system sender and receiver share a single key which is used to encrypt and decrypt a message. It is also called secret key cryptography. The algorithms used for symmetric – key cryptography is called symmetric- key algorithms. There are two types of symmetric algorithms such as stream cipher and block cipher. Stream ciphers encrypt the bits of information one at a time and Block ciphers encrypt the information by breaking down into blocks [6].
List of Symmetric Algorithms
• Data Encryption Standard (DES)
• Advanced Encryption Standard (AES)
• Blowfish Encryption Algorithm
• International Data Encryption Algorithm
• Triple Data Encryption Standard etc.

2. Asymmetric – key cryptography:
In Asymmetric Cryptography, two different keys are used for encryption and decryption- Public and Private. The public key is meant for general use so it is available to anyone on the network. Anyone who wants to encrypt the plaintext should know the Public Key of receiver. Only the authorized person can be able to decrypt the cipher text through his own private key [6].
Private Key is kept secret from the outside world.
List of public – key algorithms
• Diffie-Hellman
• RSA
• DSA etc.
Symmetric Encryption Algorithm runs faster as compared to Asymmetric key algorithms. Also the memory requirement of Symmetric algorithm is lesser as compared to asymmetric.

1.4 Fuzzy Logic Concept

Fuzzy Logic is basically a multivalued logic that allows intermediate values to be defined between conventional evaluations like yes/no, true/false, black/white, etc. and a continuous range of truth values in the interval notions like rather warm or pretty cold can be formulated mathematically and processed by computers[10].

Give a Relation R, representing the controller, and a relation A', representing the controller input, a fuzzy output B', can be obtained by the composition of A' and R: [19]
B'=A'O R'

However, the in-and outputs of a controller are normally numerical values, so a translation is necessary from the numerical inputs to a fuzzy input, and a translation from the fuzzy output to numerical outputs. The first translation is known as Fuzzification, the latter as Defuzzification. A schematic representation of a fuzzy controller is given in figure [19].

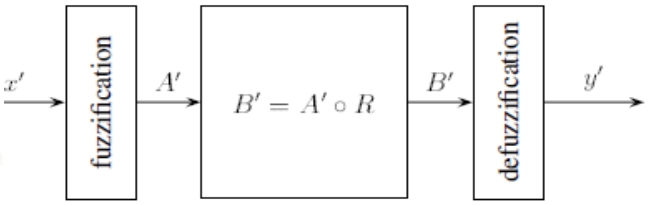


Figure 1: Fuzzification and Defuzzification Process

1.5 Fuzzy Logic Benefits:

- Simplified and reduced development cycle.
- Ease of implementation.
- Can provide more "user- friendly" and efficient performance.

1.6 Fuzzification

Fuzzification is the process of making a crisp quantity fuzzy. We do this by simply recognizing that many of the quantities that we consider to be crisp and deterministic are actually not deterministic at all: They carry considerable uncertainty. If the form of uncertainty happens to arise because of imprecision, ambiguity, or vagueness, then the variable is probably fuzzy and can be represented by a membership function [11] [19].

1.7 Defuzzification

Defuzzification is the process of producing a quantifiable result in fuzzy logic, given fuzzy sets and corresponding membership degrees. It is typically needed in fuzzy control systems. These will have a number of rules that transform a number of variables into a fuzzy result, that is, the result is described in terms of membership in fuzzy sets [12].

1.7.1 Defuzzification to Scalar
Defuzzification is the conversion of a fuzzy quantity to a precise quantity, just as Fuzzification is the conversion of a precise quantity to a fuzzy quantity [19].

1.7.2 Defuzzification To Scalars Methodes
1. Max membership principle.
2. Centroid method.
3. Weighted average method.
4. Mean max membership (middle-of-maxima).
5. Center of sums.
6. Center of largest Area.
7. First (or last) of maxima.

2. Literature Survey

Licensed Under Creative Commons Attribution CC BY

Advantages:
- Blowfish is significantly faster than DES, AES and 3DES [6].
- Consume less memory than DES, AES and 3DES [5].
- it is suitable & efficient for hardware implementation [5].
- If we change key size, there is no affect time of execution of algorithm [6].

Disadvantages:
- Size of plaintext is affect to the speed of algorithm [1].
- Suffer from weak key Generation Policy so cryptanalysis get the message by Brute force attack [6].

The parameter still left to evaluate:
- Suffer from weak key generation policy so we change the key generation policy.
- Change the type of plaintext and size of plaintext.
- Change the key size for performance.
- Possible to minimize the key size of blowfish and making round more complexes for improving performance.

3. Existing System

3.1 Methodology

Some specifications of Blowfish algorithm are as follows:
- A 64 bit blocks cipher with a variable key length.
- There is a P-array and four 32-bit S-boxes. The P-array contains 18 of 32-bit subkeys, while each S-box contains 256 entries.
- 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 totalling 4168 bytes.
- The data encryption occurs via a 16-round Feistel network. Each round consists of a key-dependent permutation, and a key and data-dependent substitution.
- All operations are XORs and additions on 32-bit words.
- The input is a 64 bit data element.

The process of Sub key generation is illustrated as follows-
1. Initialize P array and S boxes with Hexadecimal digits of Pi.
2. XOR P-array with the key bits (i.e., P1 XOR (first 32 bits of key), P2 XOR (second 32 bits of key)…
3. Use the above method to encrypt the all-zero string.
4. This new output is P1 and P2.
5. Encrypt the new P1 and P2 with the modified sub keys.
6. This new output is now P3 and P4.
7. Repeat the above steps until we get all the elements of P array i.e P1, P2….

The encryption algorithm for Blowfish is illustrated as follows:

1. Divide X into two 32 –bit halves: XL, XR
2. For i=1 to 16
   XL=XL XOR Pi
   XR=F(XL) XOR XR
   Swap Xl and XR
3. Swap XL and Xr (Undo the last Swap)
4. XR=XR XOR P17
5. XL=XL XOR P18
6. Concentrate on XL and XR

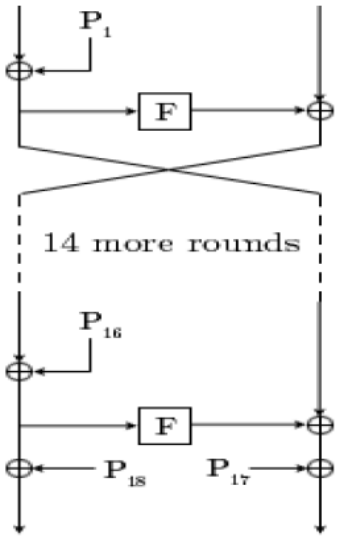


Figure 2: Blowfish each Round action

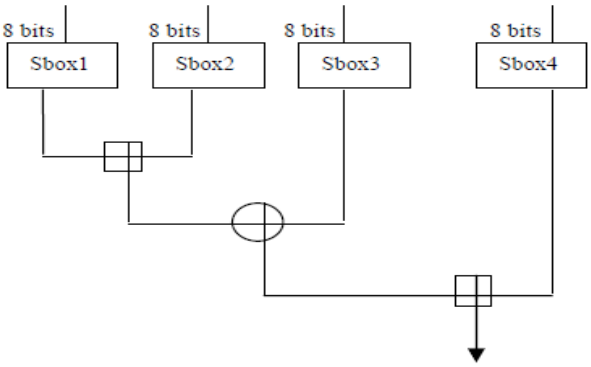


Figure 3: Working of F function

In this algorithm an F function is used which is represented by The F function uses the substitution boxes of which there are four, each containing 256 32-bit entries [10]. If the block XL is divided into 8-bit blocks a, b, c and d, the function F(XL) is given by the formula:

F(XL)= ((S1,a + S2,b mod 2^32) XOR S3,c) + S4,d mod 2^32 .

The decryption process is just reverse of the encryption process.

4. Proposed System

4.1 Encryption Algorithm

Step1: Select Image as Plaintext
Step2: Divide the image into sub images of size 10X10 pixel.
Step3: Split image pixels colour to array of Red, Green and Blue colours (RGB).
Step4: load Secret key.
Step5: Convert Key to ASCII codes.
Step6: Cipher ASCII codes by using fuzzy standard functions:

If x <= a then F(x, a, c) =0
If x>c then f(x, a, c) =1
If (a<x) and (x<= (a+c)/2) then
F(x, a, c) =2 ((x-a)/(c-a)) 2
If (((a+2)/2) <x) and (x<=c) then
F(x, a, c) = 1-2((c-x)/(c-a)) 2

Licensed Under Creative Commons Attribution CC BY

Where x refer to ASCII value, a refer to the start point and c refer to the end point
Step7: Convert the result of Fuzzy function into binary stream.
Step 8: Fuzzy Value XOR with Sub images (XL Part)
Step9: Apply this to the modified F-function.
Step10: repeat Step-8 &9 up to 16 Round.
Step11: Get Encrypted Image.

4.2 Decryption Algorithm

Step1: Load encrypted image file.
Step2: Enter Secret Key Decipher ASCII codes by using DE fuzzy standard functions:
Output=

$$\frac{\sum_i \mu_A(y_i) \times y_i}{\sum_i \mu_A(y_i)}$$

Where μ_A, y_i parameter of inverse fuzzy function
Step3: Apply result into Sub-Key Generation.
Step4: And Apply to Round Function of Modified S-Boxes Blowfish Algorithm.
Step5: get the original Image.

4.3 Modified F Function

Use of multithreading for the s-box XOR operation we can executing the operation faster compare to the original Blowfish S-Box Operation we can get better performance of Execution Time.

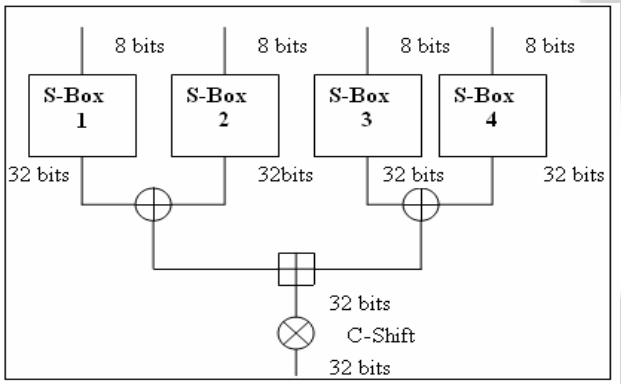


Figure 4: Proposed F Function

F (XL) = ((S1, a XOR S2, b mod 2^32) + (S3, c XOR S4, d mod 2^32))

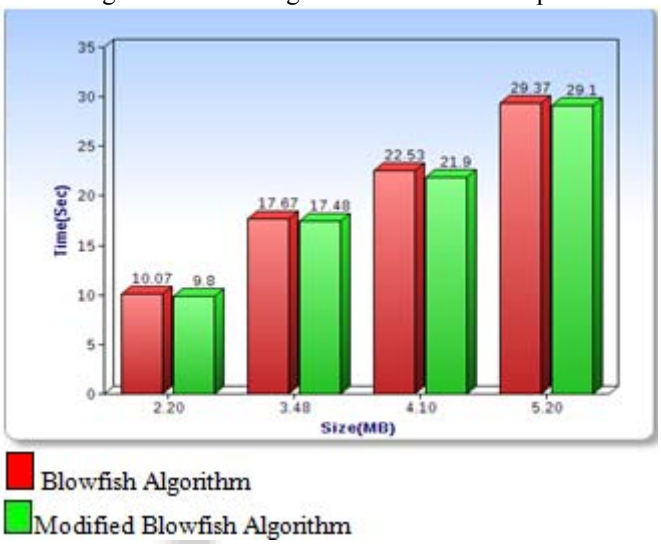
5. Result Analysis

Table 1: Comparison of Encryption Time and Decryption Time of Blowfish and Modified Blowfish Algorithm

Size (MB)	Encryption Time (Sec)		Decryption Time (Sec)	
	Blowfish Algorithm	Modified Blowfish	Blowfish Algorithm	Modified Blowfish
2.20	10.07	9.8	10.01	9.75
3.48	17.67	17.48	17.60	17.39
4.10	22.53	21.90	22.43	21.82
5.10	29.37	29.10	29.29	28.87

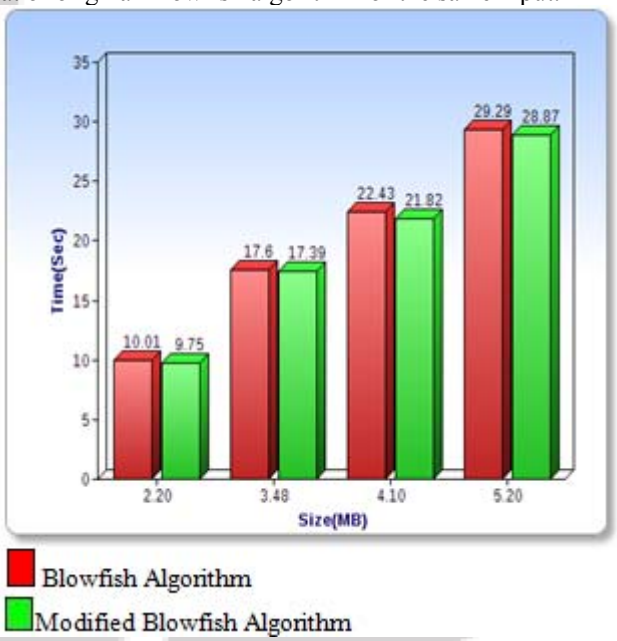
5.1 Encryption Time

They get the result the amount of encryption time taken by Modified Blowfish algorithm is almost half as compared to that of original Blowfish algorithm for the same input.



5.2 Decryption time

They get the result the amount of decryption time taken by Modified Blowfish algorithm is almost half as compared to that of original Blowfish algorithm for the same input.



6. Conclusion

Blowfish algorithm give a better Performance and more security and strongest against any type of intrusion, but the blowfish algorithm has some weakness. The most important of them is S-Boxes weakness based on collision. Weak key generation policy and some vulnerability in steps of the key generation process.

We can overcome this weakness by modifying generation of sub Keys, and changing frequently by using randomness fuzzy value which are derived by different fuzzy set of condition, after modify algorithm we are applying encryption

Licensed Under Creative Commons Attribution CC BY

& decryption on image. so we get the strong key for encryption and Improved a Performance of Execution time and a security of generation of key using fuzzy value and the use of fuzzy value we get a secure and fast computation for key.

7. Future Work

Blowfish algorithm give a better Performance and more security and strongest against any type of intrusion, but the blowfish algorithm has some weakness. The most important of them is S-Boxes weakness based on collision. Weak key generation policy and some vulnerability in steps of the key generation process.
We can make stronger and secure the system by making more fuzzy rules and making System more secure. We will also work on Plaintext Size and Type.

New Approach of Fuzzy value into Security Make the system Problem Solving. Fuzzy values use into the LSB Technique for the image and then apply that Steno-image to the modified blowfish algorithm for image encryption, and we get the two level Higher Security and the improved Performance.

8. Acknowledgments

With the cooperation of my guide, I am highly indebted to **Asst. Prof. Neha Parmar**, for his valuable guidance and supervision regarding my topic as well as for providing necessary information.

References

[1] Asaf M.Ali Al-Neaimi, Rehab F. Hassan, "New Approach for Modifying Blowfish Algorithm by Using Multiple Keys", International Journal of Computer Science and Network Security (IJCSNS), VOL.11 No.3, March 2011
[2] Gurjeevan Singh, Ashwani Kumar, K.S Sandha "A Study of New Trends in Blowfish Algorithm", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Volume 1, Issues 2
[3] Irfan.Landge, Burhanuddin Contractor, Aamna Patel and Rozina Choudhary "Image encryption and decryption using blowfish algorithm", World Journal of Science and Technology 2012, 2(3):151-156 ISSN: 2231 – 2587
[4] Monika Agrawal, Pradeep Mishra, "A 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
[5] A.Ramesh, Dr.A.Suruliandi "Performance Analysis of Encryption Algorithms for Information Security", International Conference on Circuits, Power and Computing Technologies IEEE 2013
[6] Komal Patel,Sumit Utareja,Hitesh Gupta "Information Hidding Using Least Signifiacant Bit Stegnography and Blowfish Algorithm", Intenational Journal of Computer Applications (0975-8887) Volume63-No.13,Febuary 2013.
[7] OP Verma,Ritu Agrwal,Dhiraj Dafouti,Shobha Tyagi,"Performace Analysis Of Data Encryption Algorithm" IEEE 2011
[8] Ajit Singh,Swati Malik "Securing Data by Using Cryptography with Steganography", International Journal of Advanced Research in Computer Science and Software Engineering(IJARCSSE) ISSN: 2277 128X, Volume 3, Issue 5, May 2013.
[9] S.D. Kaelhler, " Fuzzy Logic and Fuzzy Control", Seattle Robotics Society, 2005.
[10] Bonde, "Fuzzy Logic Basics", GTE Government System Corp., Needham, MA 02194,2000.
[11] N. H. Mateou ,A. S. Andreou ,George A. Zombanakis " Fuzzification and Defuzzification Process in Genetically Evolved Fuzzy Cognitive Maps (GEFCMs)" 8th WSEAS International Conference on Circuits, Systems, Communications and Computers (CSCC), (14. July 2004)
[12] http://en.wikipedia.org/wiki/Defuzzification
[13] https://oit.unlv.edu/network-and-security/definition-information-security
[14] Russell K. Meyers, Ahmed H. Desoky "An Implementation of the Blowfish Cryptosystem", IEEE,2008
[15] Ashwak ALabaichi, Faudziah Ahmad, Ramlan Mahmod "Security Analysis of Blowfish algorithm",IEEE, ISBN: 978-1-4673-5256-7/13,2013
[16] http://crypto.stackexchange.com/questions/2338/big-o-notation-encryption-algorithms
[17] William Stallings, Cryptography and Network Security, Fifth Edition, Pearson Education, Inc., 14th January 2010
[18] Ren´e Jager," Fuzzy logic in control",Technische University,Dutch, ISBN 90-9008318-9,1995
[19] T. J. Ross, Fuzzy Logic with Engineering Applications, Second Edition, 2004
[20] Orhun Kara, Cevat Manap "A New Class of Weak Keys for Blowfish", 14th International Workshop, Luxembourg, March26-28,2007

Licensed Under Creative Commons Attribution CC BY