American Journal of Engineering Research (AJER)
e-ISSN : 2320-0847 p-ISSN : 2320-0936
Volume-3, Issue-7, pp-161-166
www.ajer.org

Research Paper Open Access

Comparison of Blowfish and Cast-128 Algorithms Using Encryption Quality, Key Sensitivity and Correlation Coefficient Analysis

Shailaja S[1], Dr Krishnamurthy G N[2]
[1] *(Department of Computer Science and Engineering, PDA College of Engineering, Gulbarga, India,*
[2] *(Department of Information Science and Engineering, B N M Institute of Technology, Bangalore, India,*

ABSTRACT : This paper demonstrates the performance of well known block ciphers Blowfish and Cast-128, considering different aspects of security namely, Encryption quality, Key sensitivity test and Statistical analysis. Statistical analysis is conducted using images by test on the histogram of encrypted images and correlation of horizontally adjacent pixels in an encrypted image.

KEYWORDS: Avalanche, Correlation Coefficient, Decryption, Encryption, Encryption Quality, Key Sensitivity.

I. INTRODUCTION

Blowfish [1] is a variable-length key [2], 64-bit block cipher developed by Bruce Schneier. The algorithm consists of two parts namely a key-expansion part and a data- encryption part. Key expansion converts a key of utmost 448 bits into several sub key arrays totaling 4168 bytes. Data encryption occurs via a 16-round Feistel network [1]. Each round consists of a key-dependent permutation, a key and data-dependent substitution. All operations are EX-ORs and additions on 32-bit words. CAST-128 [2], [3], [4] is a design procedure for symmetric encryption algorithm developed by Carlisle Adams and Stafford Tavares. CAST has a classical Feistel network consisting of 16 rounds and operating on 64-bit blocks of plaintext to produce 64-bit blocks of cipher text. The key size varies from 40 bits to 128 bits in 8-bit increments.

II. ENCRYPTION QUALITY

In this Subsection Encryption Quality (EQ) [5], [6] of both Blowfish and Cast-128 are calculated for digital images. Let F and F′ denote the original image and the encrypted image respectively each of size M*N pixels with L grey levels. F(x, y), F′(x, y) ε {0... L −1} are the grey levels of the images F and F′ at position (x, y) ($0 \le x \le M-1$, $0 \le y \le N-1$). Let $H_L(F)$ denote the number of occurrences of each grey level L in the original image F. Similarly, $H_L(F')$ denotes the number of occurrences of each grey level L in the encrypted image F′. The EQ represents the average number of changes to each grey level L and is expressed mathematically as:

$$Encryption\ \ Quality = \frac{\sum_{L=0}^{255} \left| H_L(F') - H_L(F) \right|}{256}$$

The effect of number of rounds r on the encryption quality for Blowfish and Cast-128 is investigated. The block size and secret key lengths are both constants. The encryption quality (EQ) is computed as a function of number of rounds (r). Fig 1, 2 and 3 show the results of Encryption and Decryption. The results obtained for the image Butterfly (AV1.bmp) using both the algorithms are shown in Table I.

Figure 1: Original Image

Figure 2: Encrypted image

Figure 3: Decrypted Image

TABLE I: Comparison Of Encryption Qualities Of Blowfish And Cast-128 For Different Rounds

Number of Rounds	Algorithm Type	
	Blowfish	Cast-128
2	900.484	1149.00
4	1055.64	1151.27
6	1094.09	1151.40
8	1142.10	1154.42
10	1140.53	1149.54
12	1135.00	1150.13
14	1138.64	1148.98
16	1144.61	1150.35

KEY SENSITIVITY TEST : A 16-CHARACTER CIPHER KEY IS USED. THE KEY CONSISTS OF 128 BITS. A TYPICAL KEY SENSITIVITY TEST [5], [6], [11] HAS BEEN PERFORMED ACCORDING TO THE FOLLOWING STEPS:

[1] An image of Butterfly (AV1.bmp) is encrypted by using the test key ADF278565E262AD1F5DEC9 4A0B**F** 25B27 (Hex).
[2] Then one bit of the key which is selected randomly is changed .We have changed the key to ADF278 565E262AD1F5DEC94A0B**B**25B27.The same image is encrypted with the modified key. The character which is changed as a result of changing an arbitrary bit is shown in bold in test key and the modified key.
[3] Finally, the above two ciphered images, encrypted by the two slightly different keys are compared.

The result is that the encrypted image using Blowfish by the key K1 =ADF278565E262A D1F5DE C94A 0B **F**25B27 has 99.6126% of pixels differing from the encrypted image by the key K2 = ADF278565E2 62A D1F5DE C94A 0B**B**25 B27 in terms of pixel grey scale values although there is only one bit difference in the two keys. The above experiment is repeated with Cast-128 shows that 99.5903% of pixels differ when we compare the image encrypted image (encrypted with key K1) with that of key K2 in terms of pixel grey scale values. Table II shows the results of percentage difference of pixels (key sensitivity analysis) of Blowfish and Cast-128 for different rounds.

TABLE II: Comparison Of Key Sensitivity Of Blowfish And Cast-128 For Different Rounds

Number of Rounds	Algorithm Type	
	Blowfish	Cast-128
2	92.39	99.57
4	98.44	99.57
6	98.73	99.58
8	99.43	99.60
10	99.57	99.57
12	99.56	99.58
14	99.56	99.58
16	99.61	99.59

Avalanche Effect :A change in one bit of the plain text or one bit of the key should produce a change in many bits of the cipher text. This change in number of bits in the cipher text whenever there is a change in one bit of the plaintext or one bit of key is called Avalanche effect [1], [2], [11]. We have counted number of times Blowfish gives better avalanche, number of times Cast-128 gives better avalanche and the number of times both algorithm give same avalanche for different rounds. Table III gives avalanche effect due to change in one bit of key.

TABLE III: Comparison Of Avalanche Effect For Different Rounds Of Blowfish And Cast-128 Algorithms For One Bit Change In Key

Number of Rounds	Blowfish Algorithm	Cast-128 Algorithm	Both Algorithms
2	17482	9480	3038
4	13834	12367	3799
6	13818	12422	3760
8	13239	12874	3887
10	13085	12977	3938
12	13030	12925	4045
14	13016	13022	3962
16	13116	12927	3957

STATISTICAL ANALYSIS : STATISTICAL ANALYSIS OF THE DIGITAL IMAGES IS CARRIED OUT USING CORRELATION COEFFICIENT ANALYSIS.

Correlation of Adjacent Two Pixels

To determine the correlation between horizontally adjacent pixels [5], [6], [11] in an image, the procedure is as follows:

First, randomly select N pairs of horizontally adjacent pixels from an image. Compute their correlation coefficient using the following formulae:

$$E(x) = \frac{1}{N}\sum_{t=1}^{N} x_i,$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2,$$

$$\operatorname{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)),$$

$$r_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}},$$

x and y represent grey-scale values of horizontally adjacent pixels in the image. E(x) represents the mean of x values; D(x) represents the variance of x values, cov (x, y) represents covariance of x and y and r_{xy} represents correlation coefficient. To test the correlation between two horizontally adjacent pixels we have randomly selected 1200 pixels and pixels adjacent to them from original (Butterfly.bmp) and their encrypted images. Then we have calculated their correlation coefficient using the equations.

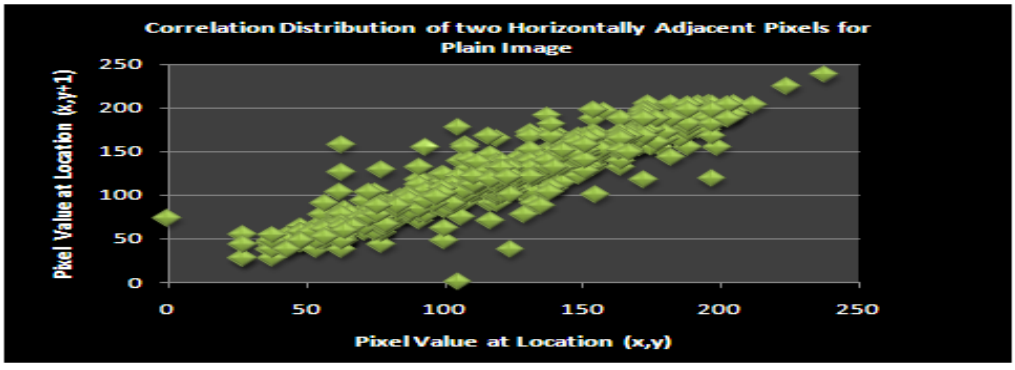

Figure 4: Correlation Distribution of Two Horizontally Adjacent Pixels for Plain Image Butterfly.bmp

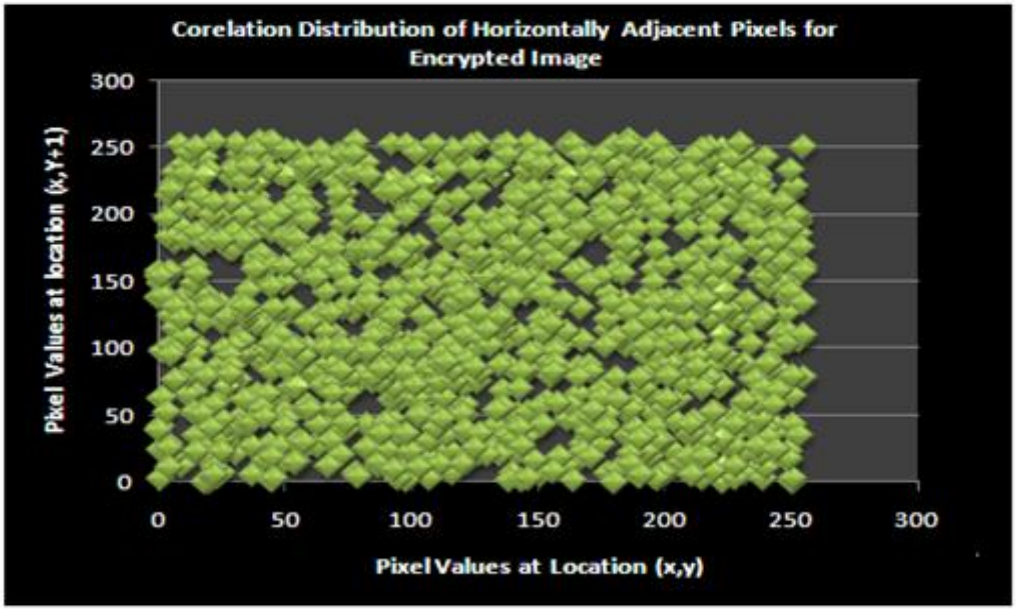

Fig.5: Correlation Distribution of Two Horizontally Adjacent Pixels for Encrypted Image Butterfly.bmp using Blowfish Algorithm.

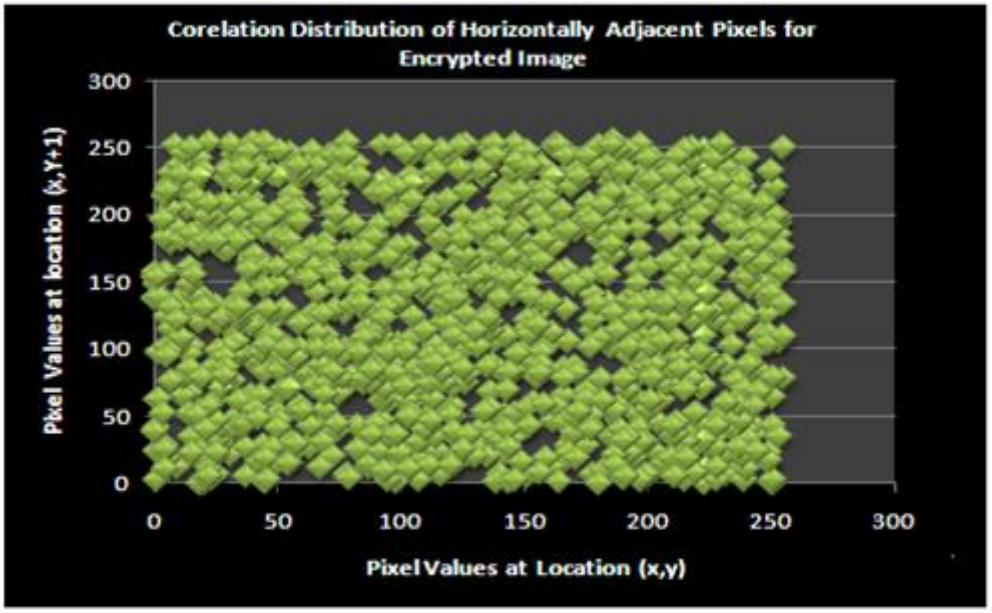

Figure 6: Correlation Distribution of Two Horizontally Adjacent Pixels for Encrypted Image Butterfly.bmp using Cast-128 Algorithm

Fig 4, 5 and 6 show the correlation distribution of two horizontally adjacent pixels in the plain image and cipher image using Blowfish and Cast-128 block ciphers. The correlation coefficient for plain image is **0.951021**. It is **0.034859** for cipher image encrypted using Blowfish and is **0.951021** for plain image and **0.00200** for cipher image encrypted using Cast-128. In cases of both original and modified algorithm the correlation coefficients for plain image with that of cipher images are far apart.

III. CONCLUSION

The results of the tests and analysis conducted in this paper lead to conclusion that the security of Blowfish Algorithm is good as compared to Cast-128 Algorithm

REFERENCES

[1] B. Schneier, “Description o f a New Variable-Length Key,64-Bit Block Cipher (Blowfish)”, Fast Software Encryption, Cambridge Security Workshop proceedings (December 1993), Springer-Verlag, 1994, pp. 191-204.

[2] B. Schneier, “Applied Cryptography: Protocols, Algorithms, and Source Code in C”, 2nd ed., John Wiley & Sons, 1995.

[3] W. Stallings, “Cryptography and Network Security: Principles and Practices”, 2nd ed., Prentice Hall, 1999.

[4] C.M. Adams, “Constructing symmetric ciphers using the CAST design procedure”, Designs, Codes, and Cryptography, Vol. 12, No. 3, November 1997, pp. 71–104.

[5] Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah, “Encryption Quality Analysis of RC5 Block Cipher Algorithm for Digital Images”, Journal of Optical Engineering, vol. 45, 2006.

[6] Hossam El-din H. Ahmed, Hamdy M. Kalash. And Osama S. Farang Allah, “Encryption Efficiency Analysis and Security Evaluation of RC6 Block Cipher for Digital Images”, International Journal Of Computer, Information, and System Science, and Engineering volume 1 number 1 2007 ISSN 1307-2331. pp 33-38.

[7] B.Schneier, “The Blowfish Encryption Algorithm”, In Dr Dobb’s Journal, pp. 38-40, April 1994.

[8] Harley R. Myler and Arthur R. Weeks, "The Pocket Handbook of Image Processing Algorithms in C", Prentice-Hall, New Jersey, 1993.

[9] Krishnamurthy G N, Dr. V Ramaswamy, “Encryption Quality Analysis and Security Evaluation of CAST-128 Algorithm using digital images”, communicated to IAENG International Journal of Computer Science, 2008.

[10] Krishnamurthy G.N, Dr. V Ramaswamy, “Performance Enhancement of CAST-128 algorithm by modifying its function”, Proceedings of International Conference in CISSE 2007, University of Bridgeport, Bridgeport, CT, USA.

[11] Krishnamurthy G N, Dr. V Ramaswamy “Encryption quality analysis and Security Evaluation of Blow-CASTFish using digital images”, Communicated to International Journal of Computational Science 2008.

[12] Adams C,”The CAST-128 Encryption Algorithm”, RFC 2144, May 1997.