Performance Test of Avalanche Effect on CRB Algorithm

Chetan Rathod[1], Prof. (Dr.) Atul Gonsai[2]

Vivekanand College for Advanced Computer and Information Science, VNSGU, Surat[1]
Dept. of Computer Science, Saurashtra University, Rajkot[2]

rathodchetan@yahoo.co.in[1], amgosai@sauuni.ernet.in[2]

Abstract

In this era of digitalization, everything is transfer on the internet. Some of the files need to have higher security. To provide security, encryption techniques play a vital role. [1] To obtain high efficiency in encryption techniques many factors play an important role. [2, 3, 16] Avalanche effect is one of the most important factors which is calculated as number of flipped bits by small change in key, or plaintext or initialization vector.[5-7] This paper provides performance analysis of encryption techniques considering avalanche effect as a key role. One more property cipher should exhibit is completeness property.[10, 11]

Keywords:

Avalanche, Security, cipher, encryption, bits

Introduction:

In digital era data security is a major concern. For achieving data security, encryption is used in large extent. Selection of efficient encryption technique depends on evaluation parameters such as time taken, avalanche effect, power consumption. [4, 8, 9] This paper focuses on avalanche effect and strict avalanche criterion parameter for CRB algorithm. CRB algorithm includes a modified Feistel network that is comparable to the original Feistel network that is included with the genetic algorithm and mutation concepts. Unlike the original Feistel network, where the values in the S-box and the XOR operation of the S-box values are identical, the genetic crossover with the new machine produced internal key and the flip bit mutation were added in order to enhance the quality of encryption. A strong avalanche effect indicates, a single bit change on the input propagates speedily throughout the encryption process or hash function, creating a certain degree of randomness in the cipher or hash value. [6] Two slightly different inputs should yield results as different as possible from each other. Consequently, making it difficult for cryptanalysts to break the algorithm

An avalanche is a rapid flow of snow down a slope, such as a hill or mountain. In cryptography, the avalanche effect is a term associated with a specific behaviour of mathematical functions used for encryption. [12-13] Avalanche effect is considered as one of the desirable property of any encryption algorithm. A slight change in either the key or the plain-text should result in a significant change in the cipher-text. This property is termed as avalanche effect. A good encryption algorithm should always satisfy the following relation: Avalanche effect > 50%. [14]

The effect ensures that an attacker cannot easily predict a plain-text through a statistical analysis. An encryption algorithm that doesn't satisfies this property can favour an easy statistical analysis. [15] That is, if the alteration in a single bit of the input results in change of only single bit of the desired output, then it's easy to crack the encrypted text. [16] Here the following chart illustrate the bits.

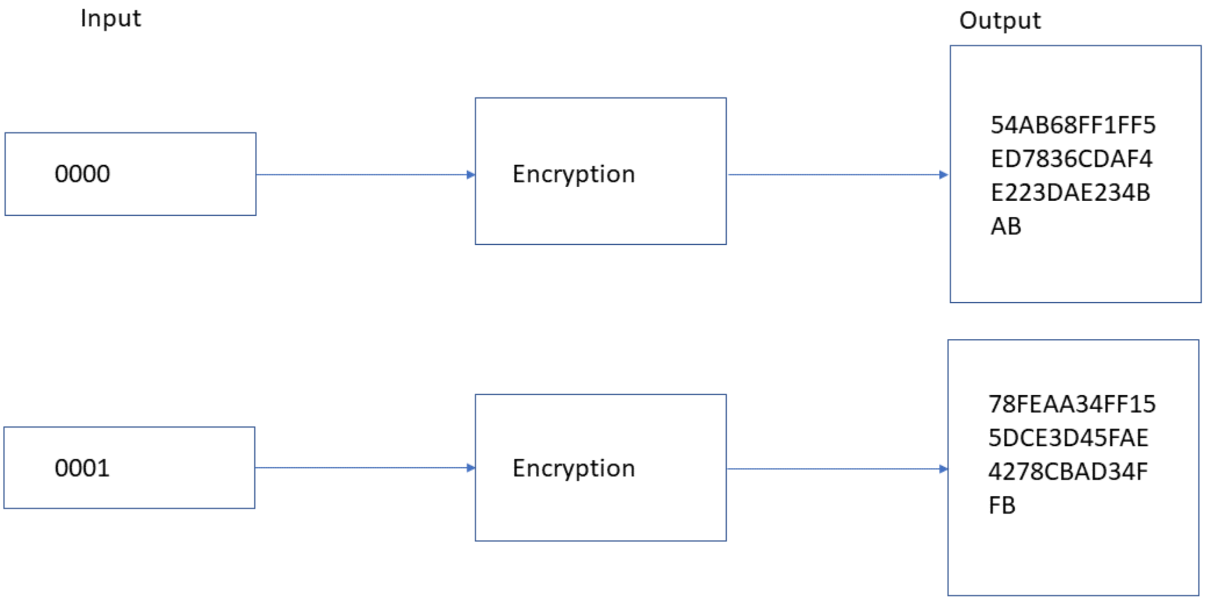


Fig 1: Encryption illustration

As shown in the figure-1. In the first phase the input key is 0000 on which the encryption is performed and got some cipher text. After changing the 1 bit in the input key and made it as 0001 and performing the same encryption algorithm on the same plain text which results in the different output. This is one of the ideal algorithms which change the huge numbers of bit after change in the single bit of the Input key. Here the avalanche effect is more than 50%, so it can be consider as the more secure algorithm for performing the encryption.

Way of counting Avalanche Effect

The avalanche effect is a phenomenon in which a small change in an input to a system leads to a dramatic change in the output. The most common way to measure the avalanche effect is to measure the number of output states that are altered when a single input is changed. This can be done by running the system with a given input and recording the output. Then, the input is changed and the output is compared to the original output. The number of states that have changed is then counted and used to measure the avalanche effect. Here the following algorithm shows the method of counting avalanche effect.

Step 1: Perform encryption using the first key on plain text and generate the cipher text.

Step 2: Perform encryption using the second key on plain text and generate the cipher text.

Step 3: Find XOR of the first and second cipher text.

Step 4: Count number of 1's in the result.

Step 5: Divide number of 1's in by the longest length of the cipher texts. Use the following formula.

$$\text{Avalanche Effect} = \frac{\mathit{Number\ of\ flipped\ bits\ in\ the\ ciphered\ text}}{\text{Number of bits in cipher ed text}} \times 100$$

For more better understanding, consider the following example. Consider that some algorithm is there for converting the plain text to cipher text.

First cipher text is : 4257871

Second cipher text is : 5687291

Result of XOR of first_cipher with second_cipher in decimal is : 0b1011000111111110110100

Total numbers of 1 is 13 which divide by length of the cipher text 25.

$$\text{Avalanche Effect} \;=\frac{13}{25}\times 100$$

Which resulted in 52 % which is the avalanche effect.

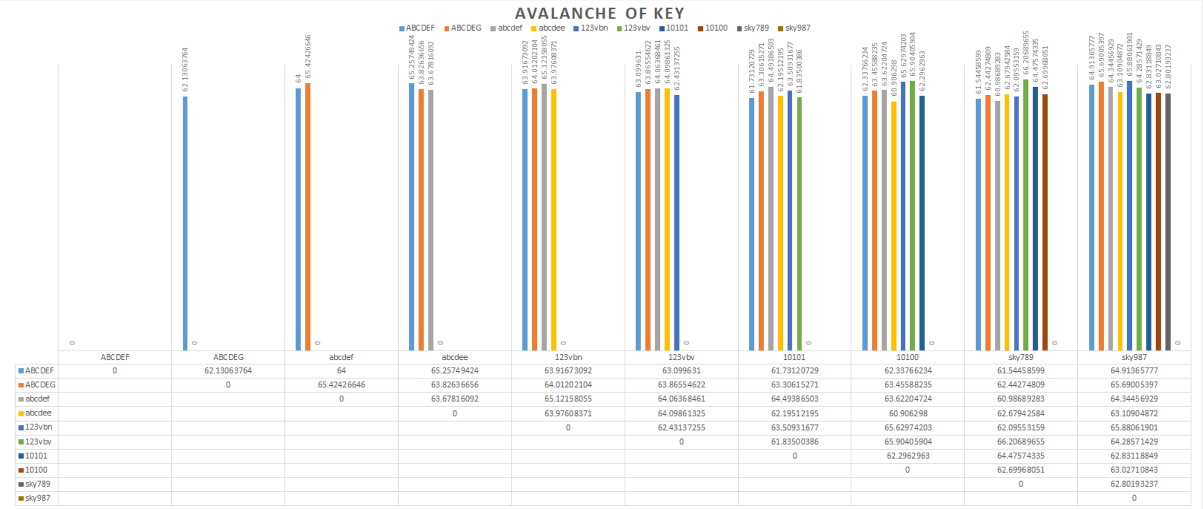
Avalanche of CRB algorithm and keys

The CRB algorithm is created on the basis of blowfish algorithm for encryption of the audio file. The CRB algorithm used different keys for the encryption and decryption process. This CRB algorithm generate one main key and 21 sub keys for the encryption and decryption process. The following table 1. describe the avalanche effect of various 10 keys generated.

KEYS	**ABCDEF**	**ABCDEG**	**Abcdef**	**abcdee**	**123vbn**	**123vbv**	**10101**	**10100**	**sky789**	**sky987**
ABCDEF	0									
ABCDEG	62.13064	0								
Abcdef	64	65.42427	0							
Abcdee	65.25749	63.82637	63.67816	0						
123vbn	63.91673	64.01202	65.12158	63.97608	0					
123vbv	63.09963	63.86555	64.06368	64.09861	62.43137	0				
10101	61.73121	63.30615	64.49387	62.19512	63.50932	61.835	0			
10100	62.33766	63.45588	63.62205	60.9063	65.62974	65.90406	62.2963	0		
sky789	61.54459	62.44275	60.98689	62.67943	62.09553	66.2069	64.47574	62.69968	0	
sky987	64.91366	65.69005	64.34457	63.10905	65.88062	64.28571	62.83119	63.02711	62.80193	0

Table 1: Avalanche value of key in %

As shown in table 1. All the 10 key compared with each other and almost in all the cases avalanche value is more then 62%. An average value of avalanche of the key is around 63% which indicate that method use for the key generation is highly effective. Those values are plotted in the figure 2.



	ABCDEF	ABCDEG	abcdef	abcdee	123vbn	123vbv	10101	10100	sky789	sky987
ABCDEF	0	62.13063764	64	65.25749424	63.91673092	63.099631	61.73120729	62.33766234	61.54458599	64.91365777
ABCDEG		0	65.42426646	63.82636656	64.01202104	63.86554622	63.30615271	63.45588235	62.44274809	65.69005397
abcdef			0	63.67816092	65.12158055	64.06368461	64.49386503	63.62204724	60.98689283	64.34456929
abcdee				0	63.97608371	64.09861325	62.19512195	60.906298	62.67942584	63.10904872
123vbn					0	62.43137255	63.50931677	65.62974203	62.09553159	65.88061901
123vbv						0	61.83500386	65.90405904	66.20689655	64.28571429
10101							0	62.2962963	64.47574335	62.83118849
10100								0	62.69968051	63.02710843
sky789									0	62.80193237
sky987										0

Figure 2: Avalanche effect of CRB algorithm key.

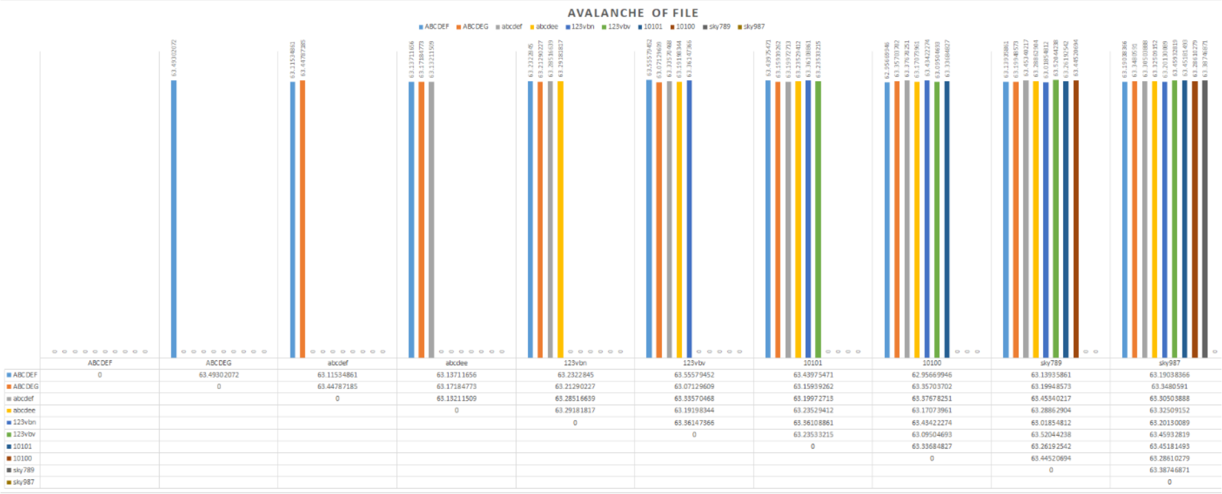
As shown in the figure 2, all the keys are compared with each key and generating output almost around 63%.

For more advance testing, this avalanche effect is counted on file. To do so, 10 keys are generated and used on the same file for the encryption process which create 10 different encrypted file of a single mp3 file. Then those 10 files are compared with each other and avalanche effect is found which is shown in the table 2.

KEYS	ABCDEF	ABCDEG	abcdef	Abcdee	123vbn	123vbv	10101	10100	sky789	sky987
ABCDEF	0									
ABCDEG	63.49302	0								
Abcdef	63.11535	63.44787	0							
Abcdee	63.13712	63.17185	63.13212	0						
123vbn	63.23228	63.2129	63.28517	63.29182	0					
123vbv	63.55579	63.0713	63.3357	63.19198	63.36147	0				
10101	63.43975	63.15939	63.19973	63.23529	63.36109	63.23533	0			
10100	62.9567	63.35704	63.37678	63.17074	63.43422	63.09505	63.33685	0		
sky789	63.13936	63.19949	63.4534	63.28863	63.01855	63.52044	63.26193	63.44521	0	
sky987	63.19038	63.34806	63.30504	63.32509	63.2013	63.45933	63.45181	63.2861	63.38747	0

Table 2: Avalanche effect on encrypted file

As shown in table 2, All the 10 files compared with each other and almost in all the cases avalanche value is more then 63%. An average value of avalanche of the key is around 63.20% which indicate that method use for the encryption is highly effective. Those values are plotted in the figure 3.



	ABCDEF	ABCDEG	abcdef	abcdee	123vbn	123vbv	10101	10100	sky789	sky987
ABCDEF	0	63.49302072	63.11534861	63.13711656	63.2322845	63.55579452	63.43975471	62.95669946	63.13935861	63.19038366
ABCDEG		0	63.44787185	63.17184773	63.21290227	63.07129609	63.15939262	63.35703702	63.19948573	63.3480591
abcdef			0	63.13211509	63.28516639	63.33570468	63.19972713	63.37678251	63.45340217	63.30503888
abcdee				0	63.29181817	63.19198344	63.23529412	63.17073961	63.28862904	63.32509152
123vbn					0	63.36147366	63.36108861	63.43422274	63.01854812	63.20130089
123vbv						0	63.23533215	63.09504693	63.52044238	63.45932819
10101							0	63.33684827	63.26192542	63.45181493
10100								0	63.44520694	63.28610279
sky789									0	63.38746871
sky987										0

Figure 3: Avalanche of the file

As shown in figure 3, avalanche effect of each file compares to other is more than 63% in all the case. This indicated that the algorithm is accurate and hard to hack by generating any random key or even trying cryptanalytic attack. It makes CRB algorithm the secure one.

Conclusion

From the method of avalanche effect, it clearly shows that the keys generated in CRB algorithm and the file which are generated by the encryption process are having high ratio of avalanche. That says that some change in the key will change almost 63% bits in the encryption file or key. So, it become more secure for the encryption and security of the files.

Reference

[1] S. Yang, L. Min, and E. Chen, "A 4-Dimensional Discrete Chaotic System and Application in Image Encryption with Avalanche Effects," *Proc. - 2015 Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discov. CyberC 2015*, vol. 1, no. 7, pp. 37–43, 2015, doi: 10.1109/CyberC.2015.70.

[2] S. N. Molotkov, "On the vulnerability of basic quantum key distribution protocols and three protocols stable to attack with 'blinding' of avalanche photodetectors," *J. Exp. Theor. Phys.*, vol. 114, no. 5, pp. 707–723, 2012, doi: 10.1134/S106377611203017X.

[3] S. Zhu and C. Zhu, "Image encryption algorithm with an avalanche effect based on a six-dimensional discrete chaotic system," *Multimed. Tools Appl.*, vol. 77, no. 21, pp. 29119–29142, 2018, doi: 10.1007/s11042-018-6078-2.

[4] M. Razeghi, *Technology of quantum devices*. 2010. doi: 10.1007/978-1-4419-1056-1.

[5] M. Y. El-Ganiny, H. M. ElAttar, M. A. A. Dahab, and T. A. Elgarf, "Improved coding gain of clipped OFDM signal using avalanche effect of AES block cipher," *2017 IEEE Pacific Rim Conf. Commun. Comput. Signal Process. PACRIM 2017 - Proc.*, vol. 2017-January, pp. 1–6, 2017, doi: 10.1109/PACRIM.2017.8121910.

[6] A. V. Kalach, A. S. Solovyov, S. L. Karpov, N. V. Martinovich, and G. S. Kalyuzhina, "Methods for prediction of the avalanche danger," *J. Phys. Conf. Ser.*, vol. 1902, no. 1, 2021, doi: 10.1088/1742-6596/1902/1/012071.

[7] Y. Deng, H. Shi, J. Gong, and T. Xie, "Avalanche effect performance test on AES algorithm," *2011 2nd Int. Conf. Mech. Autom. Control Eng. MACE 2011 - Proc.*, pp. 3932–3935, 2011, doi: 10.1109/MACE.2011.5987860.

[8] F. H. Nejad, S. Sabah, and A. J. Jam, "Analysis of avalanche effect on advance encryption standard by using dynamic S-Box depends on rounds keys," *2014 Int. Conf. Comput. Sci. Technol. ICCST 2014*, vol. 2014, no. 2005, 2014, doi: 10.1109/ICCST.2014.7045184.

[9] H. Shi, Y. Deng, and G. Yu, "Analysis of the avalanche effect of the AES S box," *2011 2nd Int. Conf. Artif. Intell. Manag. Sci. Electron. Commer. AIMSEC 2011 - Proc.*, pp. 5425–5428, 2011, doi: 10.1109/AIMSEC.2011.6009935.

[10] K. Mandal and A. Tiwari, "Comparative Stu udy of Avalanche Effect t in DES Us sing Binary Codes," pp. 0–3, 2012, DOI: 10.1109/NCCCS.2012.6413007.

[11] S. D. Sanap and V. More, "Performance analysis of encryption techniques based on avalanche effect and strict avalanche criterion," *2021 3rd Int. Conf. Signal Process. Commun. ICPSC 2021*, no. May, pp. 676–679, 2021, doi: 10.1109/ICSPC51351.2021.9451784.

[12] R. Verma and A. K. Sharma, "Cryptography: Avalanche effect of AES and RSA," *Int. J. Sci. Res. Publ.*, vol. 10, no. 4, p. p10013, 2020, doi: 10.29322/ijsrp.10.04.2020.p10013.

[13] L. Min, L. Hao, D. Han, and H. Zang, "AN AVALANCHE BLOCK ENCRYPTION SCHEME AND CHAOTIC BLOCK PSEUDORANDOM NUMBER GENERATOR WITH APPLICATION IN THE IMAGE ENCRYPTION 1 . Schools of Mathematics and Physics University of Science and Technology

Beijing Beijing , 100083 China 2 . Schools of Automat," pp. 1843–1850, 2014, DOI: 10.1109/ICOSP.2014.7015311.

[14] L. Min and G. Chen, "A novel stream encryption scheme with avalanche effect," *Eur. Phys. J. B*, vol. 86, no. 11, 2013, doi: 10.1140/epjb/e2013-40199-7.

[15] K. Mohamed, "Analyse On Avalanche Effect In Cryptography Algorithm," *Proc. Int. Conf. Sustain. Pract. Dev. Urban. (IConsPADU 2021), 16 Novemb. 2021, Univ. Selangor (UNISEL), Malaysia*, vol. 3, no. November, pp. 610–618, 2022, doi: 10.15405/epms.2022.10.57.

[16] A. Kumar, "Effective Implementation and Avalanche Effect of AES," *Int. J. Secur. Priv. Trust Manag.*, vol. 1, no. 3, pp. 31–35, 2012, doi: 10.5121/ijsptm.2012.1303.