SECURITY ENHANCEMENT USING CUSTOM-AES AND ITS PERFORMANCE EVALUATION ON AVALANCHE EFFECT-A NEW APPROACH

R. Caroline Kalaiselvi

Research Scholar, PG and Research Department of Computer Science, Presidency College, Chennai, India
carrie.jonna@gmail.com

Dr. S. Mary Vennila

Associate Professor and Research Supervisor, PG & Research Department of Computer Science, Presidency College, Chennai, India
vennilarhymend@yahoo.co.in

Abstract-Cryptography has emerged as a critical component of an information security system's protection against malicious attacks. Cryptography is the technique or method by which a person or users sends information or a message to another person or users in such a way that only the approved person or users can read it. This encryption mechanism encrypts the data and transforms the data into unreadable text that only a party with the associated key can decode or decrypt. These algorithms use a large number of computer resources, including CPU time, memory and time of processing. This research proposes a Custom-AES algorithm for data transmission to meet different security objectives. This latest algorithm is based on the Advanced Encryption Standard's symmetric key encryption (AES). The avalanche effect is used to measure the security of the Advanced Encryption Standard (AES). Before the encryption method, plaintext and the phases of encryption underwent numerous changes. By modifying one bit in plaintext while holding the key unchanged, the Avalanche effect can be determined. The introduction of this methodology was carried out for the purpose of testing. After a comparison analysis with existing encryption algorithms, the experimental results show that Custom-AES has a significant high Avalanche impact.

Keywords: AES; Avalanche Effect; Encryption; Ciphertext; Decryption; Custom-AES.

1. Introduction

Confidential digital data delivery through communication mediums has shown the need for fast and trustworthy digital communications networks to meet the data integrity, confidentiality, and unreproduction requirements. Cryptography is a method to encrypt and authenticate transmission of data over insecure networks of communication. It enables us, without reading it by unauthorized parties, to collect and/or send confidential information via vulnerable communication networks [1].

In order to encrypt confidential information on computer networks, cryptography is an essential method. Data In order to make it unreadable and unacceptable for anyone during transmission, cryptography is the means by which the content of data such as text, images, audio and video are scratched. It is mainly aimed at encrypting data from unauthorized access [2]. Information that can be interpreted and understood is called plaintext or simple text. This approach is called encryption to scratch the plaintext. Plaintext encryption creates information called a cipher text of unreadable information. Cipher text is called decryption to convert it to original information. The complexity of the encryption process is based upon an algorithm for encryption, software and the key for encrypting or decrypting the data used in the algorithm. The safety of any encryption scheme is based on Kirchhoff's safety theory. According to Kirchhoff the security is rely not on the encryption algorithm, but on the confidentiality of the encryption/decrypting key [3].

In this age, the use of the Internet is growing quickly and many people share information both publicly and via the Internet. This leads to the need for protection, since the transmission of data and information is sensitive. One of the main steps to protect sensitive information can be found in the encryption technique. This encryption is done with conventional methods of encryption. However, there are some security shortcomings in the standard

encryption technique. Therefore, it proposes an enhanced encryption algorithm. This enhanced encryption algorithm is capable of enhancing transmission protection by scanning, improving and arranging many well-known algorithms such as AES. The analysis of the theory of cryptographic technique based on the symmetrical cryptograph function proposes a new enhanced AES concept. In addition, the safety and performance of the procedure proposed is also assessed. In the conventional AES algorithm, changes are made to enhance security. These improvements will validate the effectiveness, and improve the existing AES would demonstrate a high degree of safety, in light of the experimental results.

2. Literature Survey

A new algorithm has been drafted, developed, enhanced "Design and Development of the New Symmetric Cryptography Protocol" [4]. It offers a confidentiality architecture for text information with a high public Avalanche effect that can be used for different software applications such as banking, medical services and many more. However, because of the large number of rounds, the encryption time is greater. The proposal was made for the design of an algorithm of high effect of Avalanche [5]. It produces a good Avalanche effect and can include some plain text during encryption. The efficiency of the classical cryptographic algorithms depends on this. Its impact of Avalanche is only around 57%. Digital communication's rapid development poses high risks of data security breaches. Triple SV[6] has a much better Avalanche effect than any other current algorithm, so it is possible to use any single text during the encryption process. It has 112 bits of key size. The main size is not adequate depending on the brute force attack. The hybrid AESDES [8] structure is present in the Enhanced cryptography algorithm [7]. The performance assessment has been carried out on the basis of a parameters: Avalanche effect [9]. In hybrid AES-DES algorithms, the Avalanche effect is stronger than other algorithms. However, only 1 round got evaluated this algorithm. Over many rounds, performance can be increased or reduced.

The Blowfish algorithm [10] results in a convincing blowfish algorithm. After every round, approximately 50% of cipher bits differ. In addition, if the plaintext is modified, the Avalanche effect is greater than the key shift. The impact of Avalanche is not sufficient to ensure good protection. Binary codes are helpful and have been shown by [11] to ensure data security. It proposes the algorithm for using different binary codes in cryptography directly instead of plaintext. It shows better than current algorithms that the Avalanche effect is. But it gives a strong Gray code Avalanche effect. The text/key input is translated into intermediate text and then into chip text. The runtime is much longer than the algorithms that exist. Cryptography is typical of confusion and diffusion.
In the image encryption scheme, the term block diffusion [12] is used. Confusion using the rotation matrix has been applied. The pixel location and the pixel values are altered during the confusion process. The intermediate data are larger than the original data during the uncertainty process. Therefore, more room must maintain intermediate data according to space complexity. In information security, mathematical and bit-wise operations play an important role.

3. Proposed System

The proposed method uses AES algorithm as AES is the safest algorithm. Some attacks on the AES algorithm are occurring like linear algebraic attacks, hence the AES is used in round structure for increasing complexity. This paper aims at improving the encryption and decryption algorithm. This paper has created the entire cryptographic architecture.
In this section an improved data transmission encryption algorithm is presented to meet the different security objectives, such as integrity, accessibility and confidentiality. A symmetric key encryption solution like AES is the basis of this new algorithm. This analyses the Advanced Encryption Standard (AES) and adds algorithm modifications by modifies cipher mode, block size, salt key size, IV key size and procedural modifications. After that, Custom-AES improved algorithm will begin to work on encryption that finally generates cipher text. The assessment of performance is carried out on the basis of parameter such as the effect of Avalanche. Figure 1 shows detailed architecture.

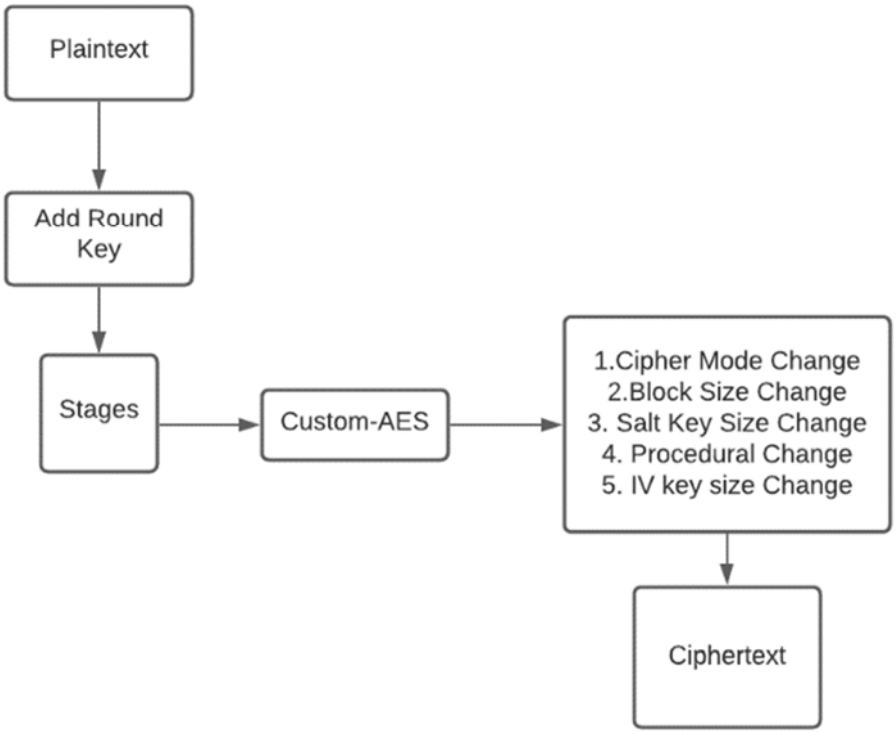

Fig.1. Block Diagram of the Proposed Custom-AES

3.1 *Model development*

The development model flow is the following:

- For the improved AES algorithm, 128-bit key length is used.
- Encryption and decryption of the proposed method are identical to standard AES algorithms.
- With the conventional AES algorithm the round process feature is identical.
- Another process of modification is undertaken in cipher mode, block size, salt key size, IV key sizes and procedural modifications.
- As a device input, we will take 256-bit data.
- These outputs then form an encrypted data block of 256 bits.

4. Results and Discussion

The changes to the AES were assessed in terms of the avalanche effect. The Avalanche effect is a useful feature of the block ciphers, which ensures that output text for a single bit is changed at least 50 percent. The execution time is the time it takes for the algorithm to encrypt or decrypt a certain input document.

4.1 *Avalanche Effect*

It is necessary to see whether the avalanche effect occurs or not to decide the security of an algorithm. Avalanche effect is an algorithm that diffuses and confuses more than 50%. The Avalanche effect is Where changing the plaintext or the key just one bit while maintaining the other constantly. It changes at least 50% of the ciphertext.. F1{i,j}n here {i,j}n meet avalanche requirements, if at least half a bit of the input bit changes to the output bit. Where I and j are bits of input and output, according to avalanche standards

$$\frac{1}{2^n}\sum_{j=1}^{n} W\left(a_j^n\right) - \frac{n}{2} \quad (1)$$

Where
$W\left(a_j^n\right) = \sum_{j=1}^{n} a_j^n$ x: {0,1}

Total change in j^{th}avalanche variable computed over whole input size 2^nin the range $0 \leq W(a_j^n) \leq 2^n$ From equation (1) we can manipulate avalanche parameter of i as

$$K_{avalanche}(i) = \frac{1}{n2^n}\sum_{j=1}^{n} W(a_j^n) - \frac{1}{2}$$

With the above formula, we proved that the probability of change of output bit when only one or bit of input is changed is half.
Also, can be defined by

$$avalanche\ Effect = \frac{number\ \ of\ bits\ flipped\ in\ cipher\ text}{number\ \ of\ bits\ in\ cipher\ text}$$

One of the main features of cryptography is the Strict Avalanche Criterion (SAC). According to the SAC, changes in 1-bit plain text affect more than half of the bits. Or, switching to a 1-bit key can affect the cipher-text more than half of the bits. The Avalanche Effect is named.
However, changing one bit of the plaintext or one bit of the key in several pieces of the cipher text can generate a shift. The Avalanche effect is called this property. The above equation can be used to measure the Avalanche Effect. Due to the one- bit fluctuation in plaintext, which keeps the encryption key constant, the output of the proposed algorithm is evaluated by means of Avalanche effect.

5. Measuring the Avalanche Effect

5.1. *Case i: Changing One character in a Word-keeping Key Constant*

The Custom-AES effect obtained a higher avalanche effect than the traditional AES algorithm based on calculated results in Table 1. The traditional AES had an avalanche of 37.03% while the Custom-AES had an avalanche of 62.9%. The number of bits flipped for Custom-AES is 17 and for conventional AES is 10.

Algorithm	Cipher1 (Encrypta)	Cipher 2(Encryptb)	Number of bits flipped	Avalanche Effect in %
Custom AES	NUNDNCI668E1DBNUEKIJSD46E UHIS	NUNDNCI668JISDYHIJNA5FFFW EF5	17	62.9
AES	SSMIBD28FKISF85USR86YNIOS6 H328	SSMIBD28FKISF85USHATSRR622 E5A	10	37.03

Table-1. Avalanche effect comparison on Custom- AES and AES by changing one character in a word keeping key constant

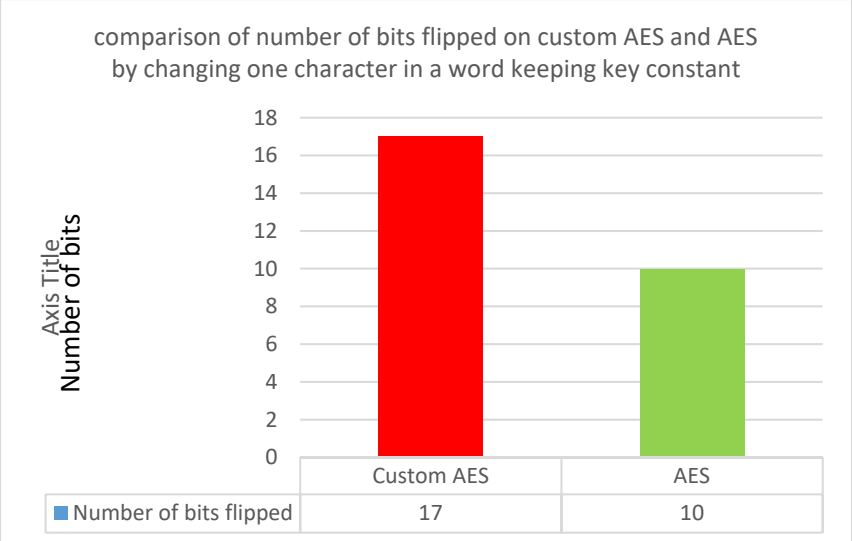

Fig. 2. Comparison of number of bits flipped on custom AES and AES by modifying one character in one word holding the key constant

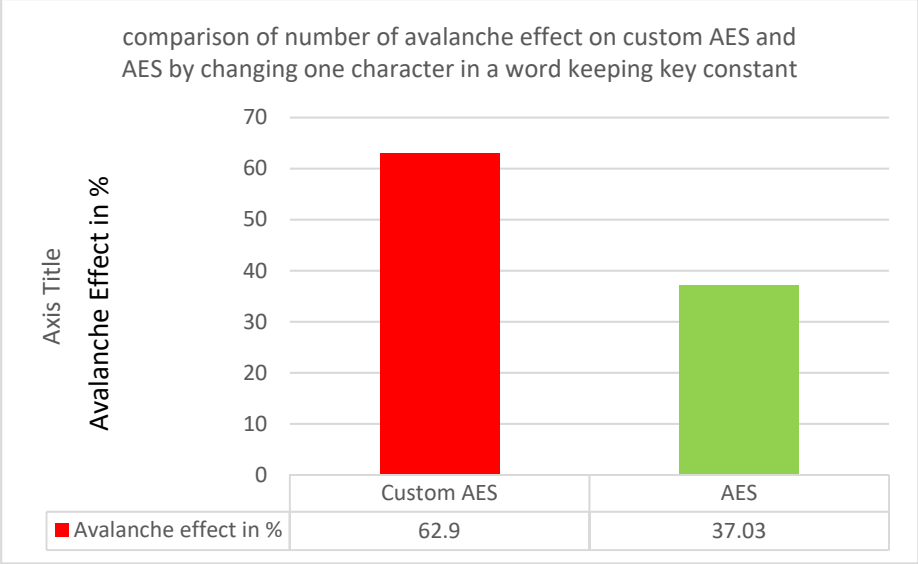

Fig. 3. Comparison of number of avalanche effect on custom AES and AES by modifying one character in a word holding the key constant

5.2. Case ii: Changing one number in a set of numbers keeping key constant

The avalanche effect achieved after changing one number in a number set is shown in Table 2. Table 2. As a result, the avalanche effect achieved by Custom-AES by 58.33% compared with the traditional AES algorithm by 33.33%. The number of bits flipped for Custom-AES is 14 and for conventional AES is 8.

Algorithm	Cipher1 (012345)	Cipher 2(012347)	Number of bits flipped	Avalanche effect in %
Custom AES	FV595SDV2DF85SD65V1V8S6D	FV595SDV2YG58DF59S5S98SD	14	58.33
AES	HYSJOD68V1SAU12G58A93A5F	HYSJOD68V1SAU12G84D8569F	8	33.33

Table 2. Avalanche effect comparison on Custom- AES and AES by changing one number in a set of numbers keeping key constant

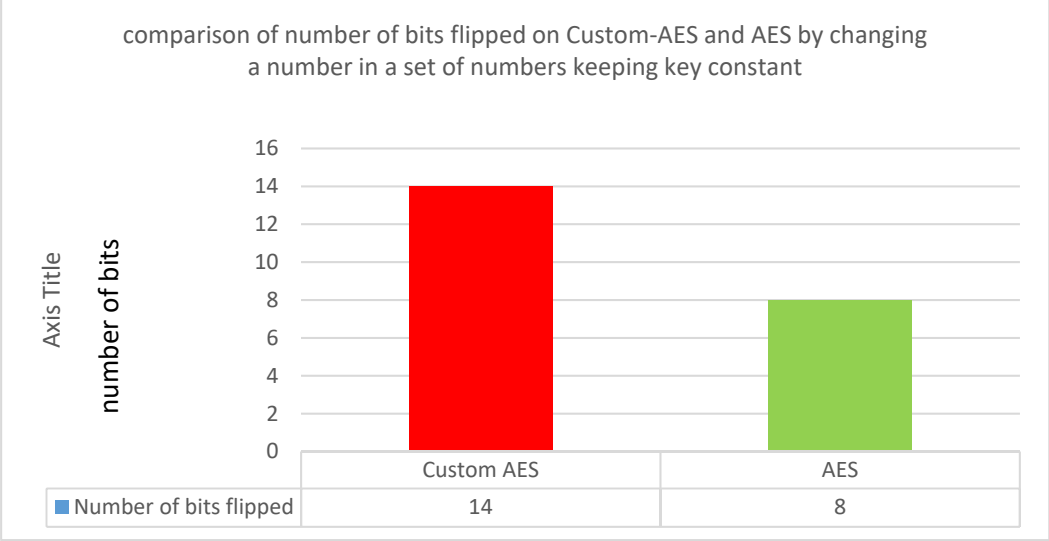

Fig. 4. Comparison of number of bits flipped on Custom-AES and AES by changing a number in a set of numbers keeping key constant

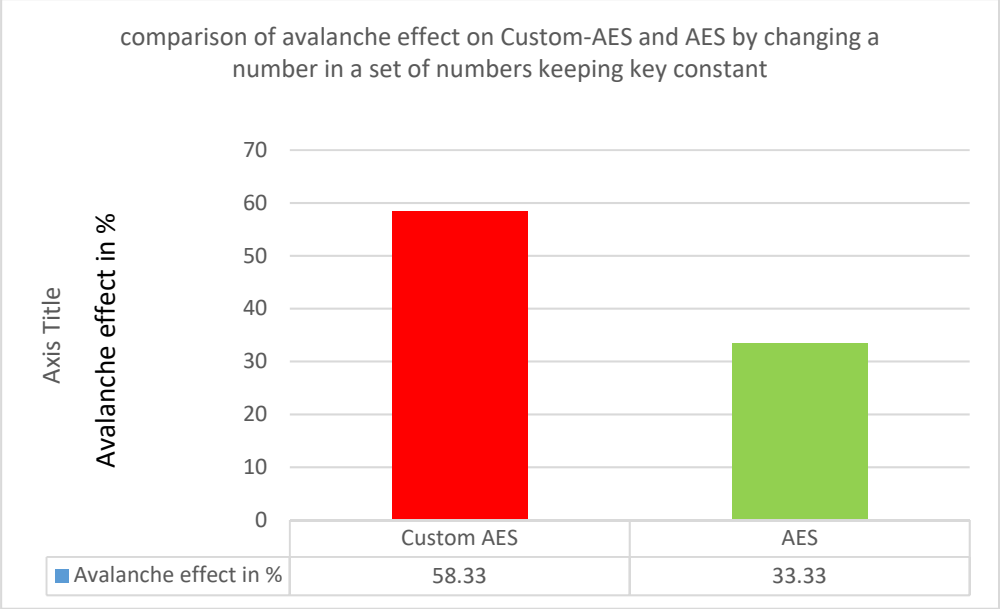

Fig.5. Comparison of the Avalanche effect on Custom-AES and AES by changing a number in a set of numbers keeping key constant

5.3. Case iii: Changing one character in a sentence keeping key constant

The conventional AES, as shown in Table 5, has an avalanche effect of 42.14%, whereas Custom-AES has an effect of 57.6%. It demonstrated a greater avalanche effect was achieved by Custom-AES. The number of bits flipped for Custom-AES is 715 and for conventional AES is 523.

Algorithm	Cipher1(Tamilnadu is my state) Total bits	Cipher2(Tamilnadu in my state) Total bits	Number of bits flipped	Avalanche effect in %
Custom AES	1241	1241	715	57.6
AES	1241	1241	523	42.14

Table3. Avalanche effect comparison on Custom-AES and AES by changing one character in a sentence keeping key constant

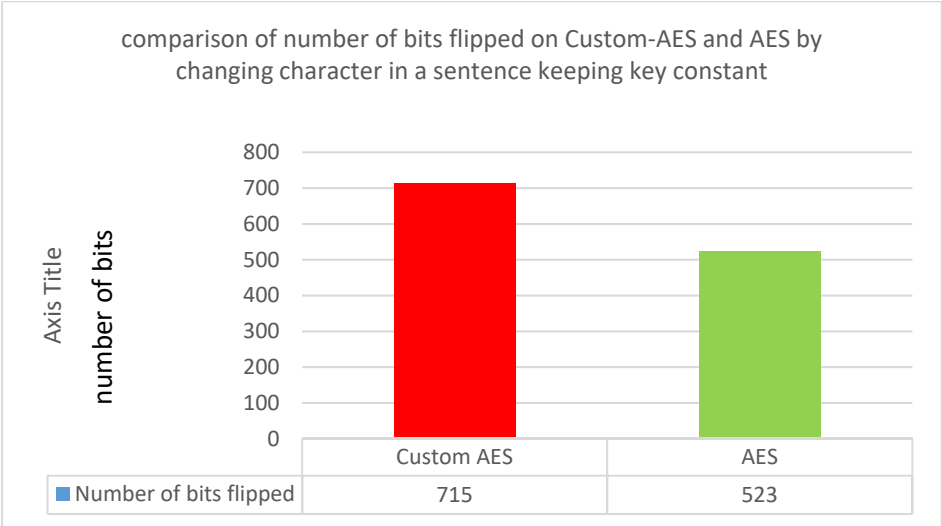

Fig.6. Comparison of number of bits flipped on Custom-AES and AES by changing character in a sentence keeping key Constant

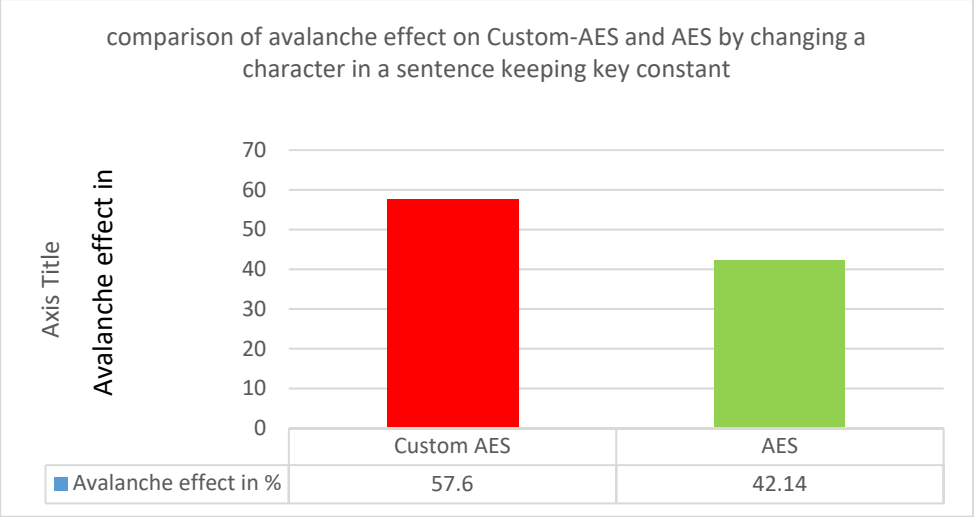

Fig. 7. Comparison of the avalanche effect on Custom-AES and AES by changing a character in a sentence keeping key constant

6. Conclusion

The method is being proposed for enhancing the traditional AES algorithm by modifying cipher mode, block size, salt key, IV key size and procedural modifications. The Custom-AES algorithm is judged by the avalanche effect and the results show the higher avalanche effect of the Custom-AES. The Avalanche Effect of the proposed method is effective and powerful from the experimental results. It supports the 256-bit block, which contributes to increased diffusion and uncertainty. The algorithm is stable. The heavy impact of avalanche. The high level of avalanche effect was reported because the traditional AES could still be improved and it is advisable to use the avalanche effect as a performance assessment method for more researchers. The proposed device is therefore good and not crackable and resistant to brute-force attacks.

Reference

[1] P.Karthigaikumar, Soumiya Rasheed"Simulation of Image Encryption using AES Algorithm" IJCA Special Issue on "Computational Science - New Dimensions & Perspectives" NCCSE, 2011
[2] Diaa Salama Abd Elminaam, Hatem Mohamad Abdual Kader,Mohiy Mohamed Hadhoud, "Evalution the Performance of Symmetric Encryption Algorithms", international journal of network security vol.10,No.3,pp,216-222,May 2010.
[3] Nidhi Singhal, J.P.S.Raina "Comparative Analysis of AES and RC4 Algorithms for Better Utilization" International Journal of Computer Trends and Technology- July to Aug Issue 2011.
[4] Prof.Gajendra Singh, Preeti Shukla, "Design and Development of New symmetric Cryptography Protocol to Improve Text Security" published by International Journal of Advanced Research inComputer Science and Software Engineering, Volume 4, Issue 11, November 2014, ISSN: 2277 128X.
[5] Debajit Sensarma, Samar Sen Sarma, "GMDES: A GRAPH BASED MODIFIED DATA ENCRYPTION STANDARD ALGORITHM WITH ENHANCED SECURITY" published by IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308, Volume: 03 Issue: 03 | Mar-2014.
[6] Sriram Ramanujam and Marimuthu Karuppiah, "Designing an algorithm with high Avalanche Effect" published by IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.1, January 2011.
[7] Rajdeep Chakraborty, Sonam Agarwal, Sridipta Misra, Vineet Khemka, Sunit Kr Agarwal, J. K. Mandal, "Triple SV: A Bit Level Symmetric Block Cipher Having High Avalanche Effect" published by (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No. 7, 2011.
[8] http://en.wikipedia.org/w/index.php?title= Confusion_and_diffusion&oldid=389143741
[9] http://en.wikipedia.org/w/index.php?title= Avalanche_effect&oldid=422317482
[10] Manisha S. Mahindrakar, "Evaluation of Blowfish Algorithm based on Avalanche Effect" published by International Journal of Innovations in Engineering and Technology (IJIET) Vol. 4 Issue 1 June 2014, ISSN: 2319-1058.
[11] Akash Kumar Mandal, Mrs. Archana Tiwari, "Analysis of Avalanche Effect in Plaintext of DES using Binary Codes" published by International Journal of Emerging Trends and Technology in Computer Science (IJETTCS) Volume 1, Issue 3, September-October 2012.
[12] Yushu Zhang, Di Xiao, "An image encryption scheme based on rotation matrix bit-level permutation and block diffusion" in Commun Nonlinear Sci Numer Simulat-Sciencedirect 19 (2014) 74-82.