International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Novel and Dynamic S-Box for Improving the Security of Audio and Video for Various Crypto - Applications

[1]Leya Elizabeth Sunny*, [2]Dr. Varghese Paul, [3]Dr. Uma Narayanan

Submitted: 21/03/2023 **Revised**: 25/05/2023 **Accepted**: 11/06/2023

Abstract: The primary objective of cryptography is to protect information from various types of security breaches. To enhance their resilience, most cryptographic techniques modify parameters such as key size, number of iterations, and incorporation of S-boxes. The only non-linear component of a substitution-permutation network is the S-box. The contents of S-boxes used in the conventional method remain constant and never undergo any changes, thus making them static. The proposed system incorporates Dynamic S-boxes, where the contents of the S-boxes change based on the key used. The values for the 8 S-boxes are created by converting the keys into their matching ASCII values. It has been discovered that the output of dynamic DES when used with audio and video data is more secure than static DES. When evaluating factors such as non-linearity, balance, implementation requirements in terms of time and memory, and the ability to resist linear and differential cryptanalysis, Dynamic S-boxes demonstrate superior performance.

Index Terms: *Dynamic DES, Non-Linearity, Balance, S-boxes, Linear Cryptanalysis, Differential Cryptanalysis.*

1. Introduction

In today's networking era, information security and privacy are major causes for concern. A system for cautious data transfer between the sender and the receiver should exist. Data security and encryption are therefore taking on increasing importance. Sensitive information needs to be secured from malicious users. The data should be transferred in a way that prevents hackers from being able to read it. Symmetric key encryption is considered as one of the primary encryption techniques for enhancing data security. Substitution and Permutation networks are utilized in the majority of contemporary ciphers to transform plain-text into a meaningless cipher utilizing a symmetric key and various numbers of rounds [1].

The complexity of a symmetric key algorithm depends on the level of strength exhibited by its S-box. Achieving Shannon's property of confusion is dependent on the S-box, which plays a critical role. An S-box generates n output bits from m input bits. There are 2^m elements with n bits a piece that makes up a m X n S-box[2].

Every round will utilize a comparable S-box, one of the two varieties of S-boxes referred to as fixed or static S-boxes. Attackers can examine a given S- Box's characteristics and find its weak points by doing so.The primary drawback of the finished square code structure is the fixed structure of the S-boxes. Data Encryption Standard (DES) S-boxes use static S-boxes. Researchers have been using the current DES, illustrated in Figure 1, for a considerable period of time. [3][4][5].

An input block gets replaced by an output block through the use of a Substitution box. The only non-linear element that causes data misinterpretation is the S-box. Images are a significant type of data. In telemedicine, medical encryption, military communications, telecommunications, etc., image encryption is widely used. The DES algorithm's flaw is that it is static by nature; regardless of the presence or absence of plain-text, the encryption process always proceeds in the same way. The DES encryption process can be changed if the plain-text encryption technique is changed [6][7].

1Cochin University of Science and Technology/ Department of Information Technology, Kochi, Kerala, 682022, India
E-mail: leyabejoy81@gmail.com
**Corresponding Author*
2Rajagiri school of Engineering and Technology/Department of Computer Science, Kochi, ,Kerala,682022,India
E-mail: vp.itcusat@gmail.com
3Rajagiri School of Engineering and Technology/ Department of Computer Science , Kochi, Kerala 682022,India
E-mail: umanithin05@gmail.com

S_1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	4	9	5	15	10	11	14	1	7	6	8	13
S_7	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Fig 1. Static DES Design

In our proposed design for Dynamic DES, as outlined in the paper, the contents of the S-boxes vary according to the key used. Therefore, distinct S-boxes are constructed for each 64-bit key. Here, a cubic function is used to translate the 8-byte key value into 8 seed values. The key values are transformed into their corresponding ASCII values, and these ASCII values are then divided by prime numbers between 100 and 1000 to create 8 seed values. The S-box's algebraic strength is assessed utilizing a variety of criteria, including the balance property, Strict Avalanche Criterion, non-linearity analysis, resistance to linear and differential cryptanalysis, and execution time and memory needs [8][9].

2. Review of Literature work

Various researchers have proposed related works concerning cryptographic techniques aimed at enhancing the security of audio and video files[10,11]. Here are some of the suggested works. To increase the potency of AES and subordinate the S-Box key, Julia et al proposed a new AES key ward. The built-in key chooses an amount to be applied to the S-box curve, whilst the second key's bytes are XORed one by one. The round key serves as the sole assessment instrument, and the outcomes are subsequently applied to remedy the S-box disturbance. So, while the S-box value is unmodified, this code framework is key-subordinate and imitates the principal AES [12][13]. In 2018, Mohammad et al. proposed a variation of AES called Variable Mapping S-box AES (VMS-AES). The AES with its innovative approach utilizes vital information about the age of the range and uses it to relocate the S-box to a more advantageous position ([21], [23], [24]). By utilizing the VMS-AES forward replacement byte changes, a shift is made concerning the boundary, a substitute boundary is added to a different confidential area, and the operation of AES sub bytes is constrained. The movement is from a specific fixed area (similar to AES) to another spot, commencing with a single byte[15]. As a result of its reliance on a secret concept, the area is also secret[17].

Data was first organized into lines within a square by Sombir Singh et al. (2013), who then randomly reorganized and read information upwards to improve the computations of the Simple Column Transposition Technique (a type of Transposition Cryptography Technique) [16]. This approach is recommended to be customized based on the nature and quantity of the material being processed. The outcome of this approach is incorporated into the DES estimation to create a scrambled version [18] [19]. The resulting text is complex and difficult to decipher, requiring additional external steps to securely handle and transmit various segments across the network [20].

Payal Patel et al. (2014) not only augmented the number of cases employed to deal with the given data, but also enhanced the key length and made the S-boxes more unpredictable, thereby increasing the overall level of unpredictability. Instead of making it simpler for monster power attacks, the key length was extended. The expert hasn't been watching the key during this evaluation[21][22].Albassali et al. (2004) suggested a technique for creating the sub-keys in the calculations employed by the GA(Genetic Algorithm)[23], which would improve the estimations. The sub-keys generated by this technique depend on the GA used, which results in a unique set of self-reinforcing sub-keys each time the application is executed. In contrast to the proposed calculation, subkeys are created from a single central key. Through the inclusion of two extra keys alongside the primary 64-digit key, Sharma et al. (2015) developed specific structures to enhance the estimation of DES. Moreover, they suggested making some changes to a few internal DES patterns that utilize S-BOX for AES computation.

From one round to the next, the S-Box AES should be altered dynamically, according to Krishnamurthy and Ramaswamy (2008). One-fourth of the core AES institutions will be governed by the welfare criteria without modifying the others. The S-box has two possible uses: The final byte from the round keys is utilized as the primary case, while in the secondary case, the S-box is combined with the bytes from both case keys through XOR operation. The manner in which the XORing is done determines the way the S-box changes between the bytes of the 2 case keys. In the third scenario, a different set of round key is employed, which are generated using a key augmentation estimate similar to that used in AES. The S-box is manipulated using the final byte of the round keys. The fourth example is similar to the third, but with the additional feature of rotating the S-box based on the subject while evaluating the large bytes of the key, and then performing XORing operations.

Mahmoud et al. (2013) suggested a distinctive version of AES-128, which employs a key-subordinate S-box that adheres to the basic S-box phase prescribed by the AES secret key. To create self-assertive groups, a pseudorandom generator (PN) called direct input shift register (LFSR) is used. By segregating two sections of the LFSR and performing XOR operation between their outputs, the AES secret key is utilized to ascertain the state of a concealed segment of the LFSR, which will be utilized for further analysis. The odd key is used to XOR the PN generator's yield. The result is transformed into hexadecimal values of 32 bits each, which are referred to as s1 and s2. On the typical S-box, the fragments and lines are changed using S1 and S2[23].

3. Work Flow of the System

The proposed dynamic DES's total workflow is shown in Figure 2, where the read key values are first transformed to ASCII key values before being sent through the whitening technique. In this case, the 8 seed values are derived from the ASCII numbers. The four rows of each S-box are produced from one of these seed values. The prime numbers between 100 and 1000 are kept in storage. In this context, determine a quantity referred to as "element" by computing the modulo-16 value of the “Seed/Prime value” [24].

If the element is still missing, then recheck for its presence and add it to the Sbox1 that is being produced. Next, if feasible, increase the prime number and form the 2nd row of Sbox1. Additionally, remember to keep the element's value, which is determined as the mod16 of ((Seed +1777)/Prime). Next, identify whether this element is present or not. If it isn’t , add the newly made Sbox1 to this element. Likewise, we will calculate the values for the 3rd and 4th rows of the associated S-box1, respectively, as mod 16 of ((Seed+2663)/Prime) and mod 16 of ((Seed+3137)/Prime), and add them. Here, follows a similar approach to create each Sbox, using a unique calculation for the "element" value, and ultimately generating eight Sboxes[14]. Figure 3 gives the Dynamic DES created using the aforementioned technique[10][11].

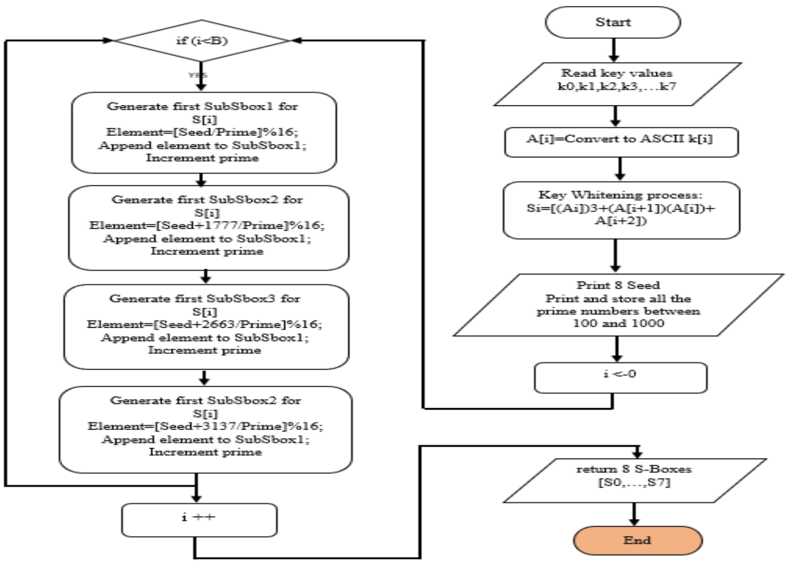

Fig 2. Workflow of Dynamic DES.

S_1

4	3	1	0	14	9	8	6	5	2	15	13	11	10	7	12
5	4	1	0	14	7	3	2	15	12	11	10	8	6	13	9
14	12	10	8	6	5	4	2	0	15	13	13	11	7	3	1
3	1	14	12	10	2	0	13	8	7	5	11	4	15	9	6

S_2

6	4	2	0	10	9	7	1	15	14	12	11	8	5	3	13
7	6	3	2	0	8	4	15	14	12	11	9	5	10	1	13
0	14	11	10	7	15	6	5	3	1	13	12	9	8	4	2
5	3	0	14	12	1	13	9	8	6	4	15	11	2	7	10

S_3

8	6	4	3	2	12	11	9	5	1	0	15	13	10	7	14
9	8	5	4	1	10	6	15	13	12	3	0	14	11	7	2
2	0	13	12	9	1	15	11	7	5	3	14	10	4	8	6
7	5	2	0	13	3	15	11	10	8	4	1	14	12	9	6

S_4

0	15	13	12	10	6	5	3	2	14	11	9	8	4	1	7
1	0	13	12	10	4	2	15	11	8	7	6	5	9	3	14
10	8	6	4	2	11	9	1	15	14	13	7	5	3	0	12
15	13	10	9	6	14	12	5	4	2	0	8	3	1	11	7

S_5

3	2	1	0	14	9	8	6	5	15	13	12	11	10	7	4
5	4	1	0	14	7	3	2	15	12	11	10	8	6	13	9
14	12	9	8	6	5	4	2	0	15	13	11	7	3	1	10
3	1	14	12	10	2	0	13	8	7	5	11	4	15	9	6

S_6

4	3	1	15	10	8	7	6	2	0	14	13	12	11	9	5
6	5	2	1	15	8	4	3	13	11	10	9	7	14	12	0
15	13	10	9	6	5	3	1	14	12	8	2	11	7	4	0
4	2	15	13	11	0	8	6	1	14	12	10	5	3	9	7

S_7

7	6	4	3	2	12	11	9	8	5	1	0	15	13	10	14
9	8	5	4	1	10	6	15	13	12	3	0	14	11	7	2
2	0	13	12	9	1	15	11	7	5	3	14	0	4	8	6
7	5	2	0	13	3	15	11	10	8	4	1	14	12	9	6

S_8

8	7	5	4	2	13	11	10	9	6	3	1	0	15	14	12
10	9	6	5	2	11	1	15	14	13	7	3	0	12	8	4
3	1	14	13	10	2	0	12	8	7	5	15	11	4	9	6
8	6	3	1	14	0	15	11	10	5	13	12	7	4	2	9

Fig 3. Developed Dynamic DES S-BOX DESIGN

4. Implementation and Results

In this section, various factors, such as the balance property manipulation, non-linearity, resistance to linear and differential cryptanalysis, as well as the time and memory requirements for execution are taken into account to analyse and discuss the effectiveness of the suggested S-box.

4.1 Balance property

A Boolean function consisting of n variables is considered balanced if the no. of input values resulting in #{x/g(x)=0} is same as the no. of input values resulting in #{x/g(x)=1}, where g(x) is the function in question. This property of balance is crucial in the context of linear cryptanalysis, where the degree of imbalance in a function can be exploited as a weakness. Therefore, balanced functions are considered strong from a cryptographic standpoint. The S-box will be more powerful if there are more balanced functions. There are 8 “6X4 S-boxes” total, and each S-box contains 64 elements. Each row has 0–15 distinct components that are not repeated.

The no. of ones and zeros in the input and output should be balanced. Our Dynamic S-boxes in both audio and video files meet the criteria for balance, an essential S-box criterion [26].

4.2 Strict Avalanche Criterion

The Avalanche criterion, also known as the requirement for a Boolean function to exhibit the property, states that as the input bits change, there should be a corresponding increase in the value of bits that are altered in the output. If a single bit complementation results in a probability of exactly one-half for the output bit to change, then the Boolean function g_n: $Z_2n \rightarrow Z_2$ is said to meet the Strict Avalanche Criterion (SAC). i.e

$$\sum_{i=0}^{2^{n}-1} g_n(v_i) \oplus g_n(v_i \oplus e) = 2^{n-1} \quad (1)$$

Where 'e' represents any element in Z_2n which has a Hamming weight of 1. If a bit changes in the input, the output bits should change by atleast half and these phenomena is called Strict Avalanche Criteria. Here we can see that the bits changed are more than half and our Dynamic S-boxes satisfy the criteria[28].

4.3 SAC using Audio files

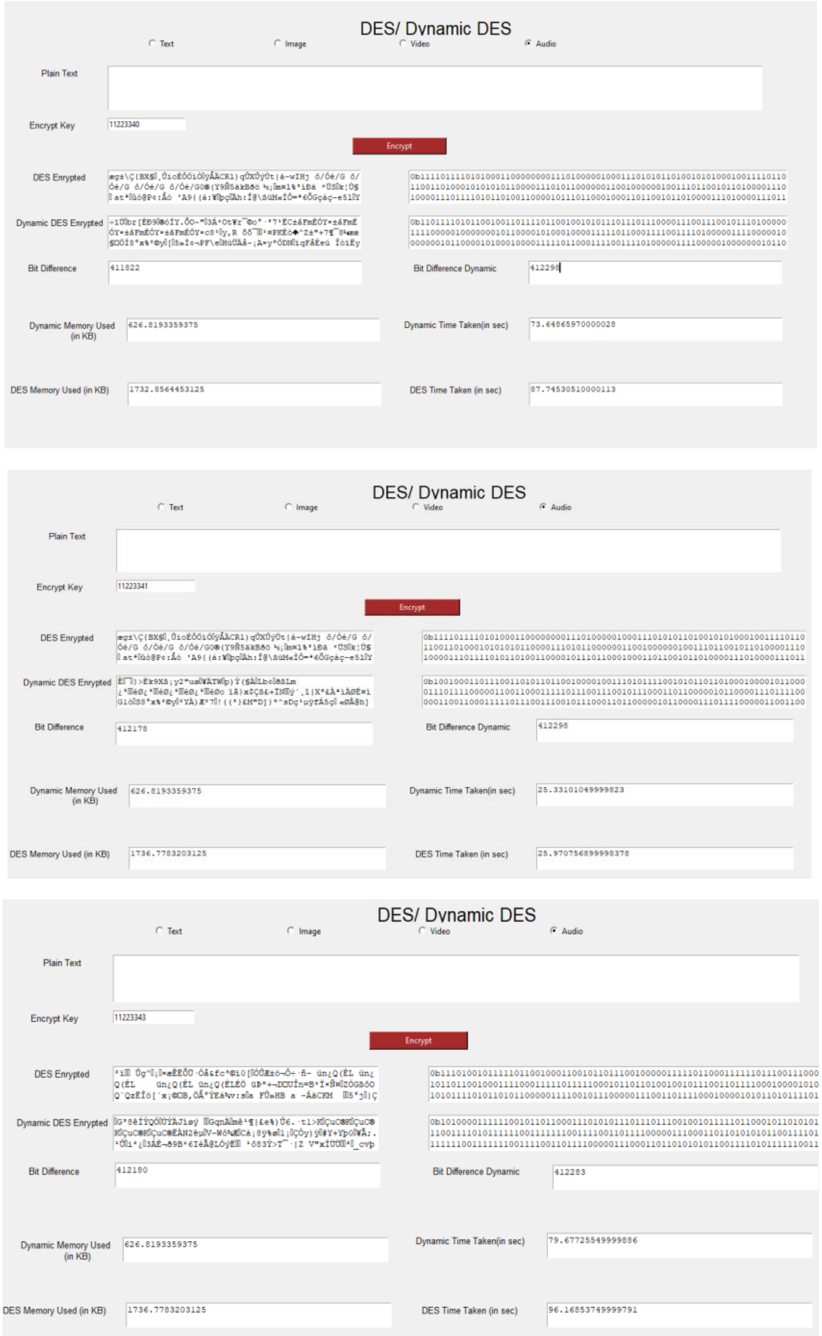

Fig 4. Bit difference using Static and Dynamic DES in Audio files

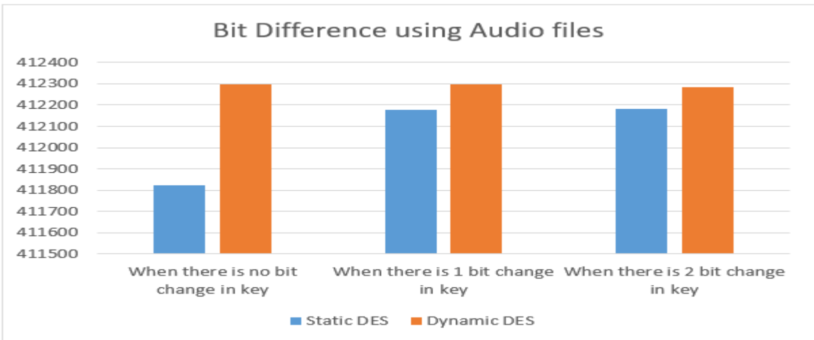

Fig 5. Comparison of Bit Difference of Static and Dynamic DES in Audio files.

Thus, from Figure 4 and Figure 5, According to [29][30], In all scenarios, Dynamic DES exhibits superior performance in terms of bit difference when compared to Static DES, as can be observed, including cases where the key remains unchanged, where there is a 1-bit change in the key, and where there is a 2-bit change in the key, specifically when analyzing audio files.

4.4 SAC Criterion using Video files

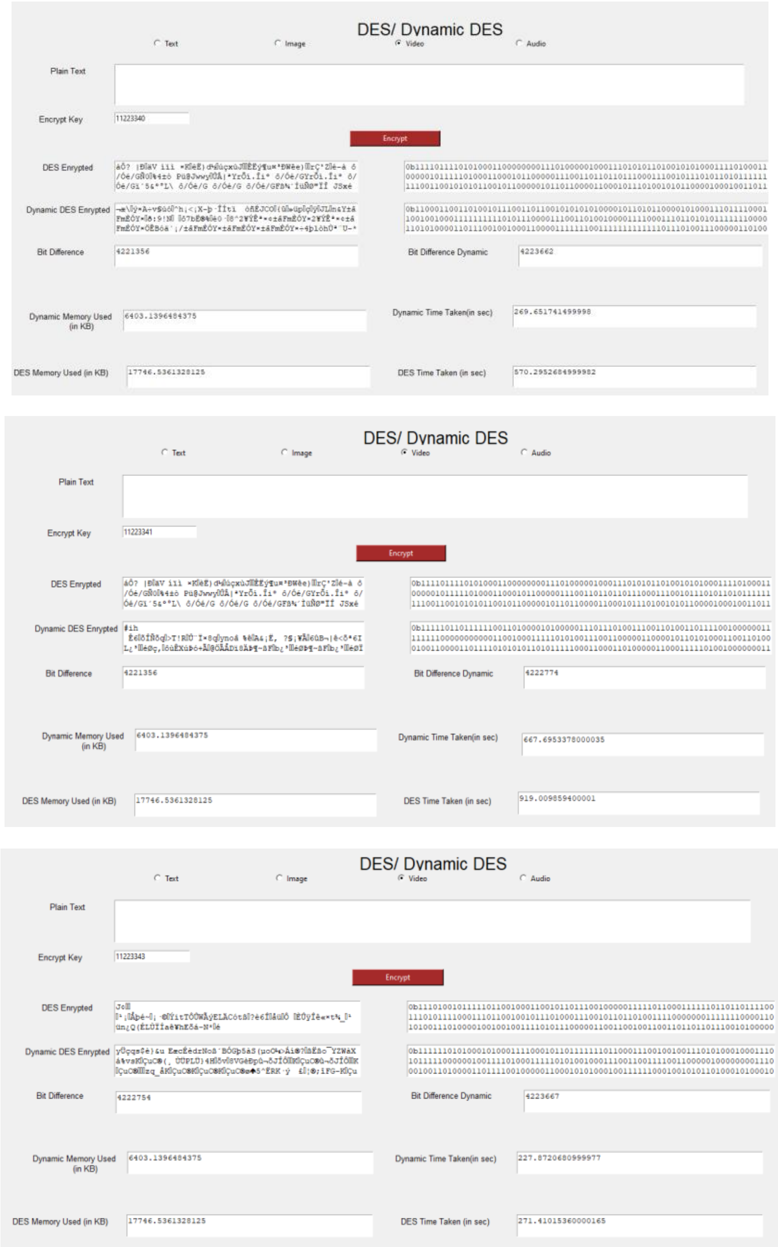

Fig 6. Bit Difference using Static and Dynamic DES in video files

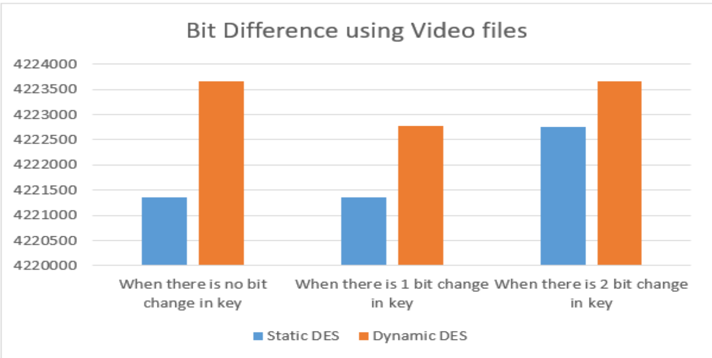

Fig 7. Comparison of Bit Difference using Static and Dynamic DES in video files.

Thus from Fig.6 and Fig.7, in all the cases, Dynamic DES outperforms Static DES when there is no bit change in key,1 bit change in key and 2 bits change in key in the case of video files[31][32].

4.5 Non-linearity

A specific number of bit changes in its truth table are required for a Boolean function to attain the closest affine function. This is known as nonlinearity. By deducting the maximum absolute distance from the predicted value and dividing the result by the value of bits in the boolean function, this number is calculated. The output cannot be expressed as a linear combination of the input bits, which is a requirement specified, thus indicating that the input-output relationship must not be linear. At all costs, it must be impossible for the hacker to separate the plain text from the ciphertext[33].

Boolean function's non-linearity N_f represents the closest distance to an affine function. It is shown by applying eq (i),

$$N_f = \frac{1}{2}\left(2^N - WHT_{max}(f)\right) \qquad (2)$$

The Walsh Hadamard Transform (WHT) is used to calculate the highest absolute value. It'll be explained as

$$WHT_{max}(f) = |F_f(a)| \qquad (3)$$

The WHT of a Boolean function f is derived by

$$\hat{F}_f(a) = \sum_{x \in B^N} \hat{f}(x)\, \hat{L}_{a(x)} \qquad (4$$

Where,

$$\hat{f}(x) = (-1)^{f(x)} \qquad (5)$$

When N is even, the S-box in GF(28) has the highest possible nonlinearity, which is given by

$$N_{max}(N) = 2^N - 2^{\frac{N}{2}-1} \qquad (6)$$

The ideal number is 120 for S-boxes in GF (2^8), while it is 28 for S-boxes in GF (2^6). Figure 8 illustrates a comparison of Dynamic DES and Static DES according to the "non-linearity" component of encrypting audio files. The non-linearity numbers for Dynamic S-boxes are evident in Figure 8, with values of 23, 21.5, 21.2, 21.21, 21.21, and 23. In contrast, the non-linearity numbers for Static S-boxes are 19.5, 19.5, 21.22, 20.20, 18.5, and 21, as indicated in the same figure. As a result, it is clear that when employing audio data, dynamic DES surpassed static DES in terms of non-linearity in all circumstances. When encrypting audio files, the non-linearity of a Dynamic S-box makes it a crucial component for a strong encryption method, making it much more secure than static S-boxes [34].

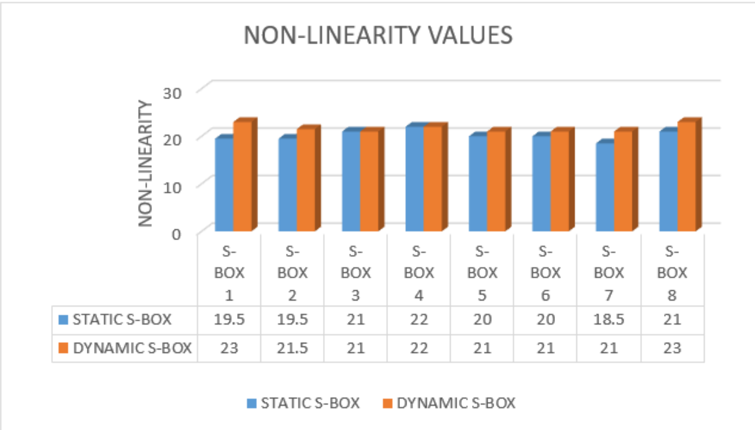

Fig 8. Comparison of non-linear numbers of Static and Dynamic DES.

Thus from Fig.8, it is understood that for audio files, the non-linearity values of the Dynamic S-box are stronger than those of the Static S-box. The following figure (Fig.9) shows the screenshots of the first dynamic S-box under the factor of non-linearity. Similarly, generate the screenshots of other S-boxes and calculate non-linearity of the entire system[35].

S-box – 1

```
FOR X1
TT:
0000000011101000010111111110011110101111011000010100101110010100
SEQUENCE:
 1 1 1 1 1 1 1 1 -1 -1 -1 1 -1 1 1 1 1 -1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 -1 -1 -1
-1 1 -1 1 -1 -1 -1 -1 1 -1 -1 1 1 1 1 -1 1 -1 1 1 -1 1 -1 -1 -1 1 1 -1 1 -1 1 1
ANF:
0000000000000000000000000000000000000000000000000000000000000000
WHT:
0, 0, -4, 4, 4, -4, -8, 8, 0, 0, 4, -4, 20, 12, 0, 0, 12, -12, 0, 0, -8, -8, 4, 12, 4, -4, 0, 0, 0, -16, 4, -20,
0, 0, -4, 4, -4, 4, 0, 0, 16, 16, 4, -4, -4, 4, 8, -8, 20, -4, -8, -8, -8, 8, 4, -4, 12, 4, 8, 8, 0, 0, -12, 12
NL: 22.0
WEIGHT: 32
DEGREE: 0
TERMS: 0
BALANCE: True

FOR X2
TT:
1101000011010010110110100001111010100101100010110001111001110001
SEQUENCE:
 -1 -1 1 -1 1 1 1 1 -1 -1 1 -1 1 1 -1 1 -1 -1 1 -1 -1 1 -1 1 1 1 1 -1 -1 -1 -1 1 -1
1 -1 1 1 -1 1 -1 -1 1 1 1 -1 1 -1 -1 1 1 1 -1 -1 -1 -1 1 1 -1 -1 -1 1 1 1 -1
ANF:
0011000000000000000000000000000000000000000000000000000000000000
WHT:
0, 0, 0, -8, -4, 12, -4, -12, 0, 0, -8, 0, -4, -4, 4, -4, 4, -4, -4, -4, -8, -16, -16, 0, 4, 12, 4, 4, -8, -16, 8,
0, 0, -8, 0, -12, 20, -4, -12, 0, 0, 0, -8, -12, 4, -12, 12, 4, 12, 4, 4, -16, 8, 0, 0, 4, -4, -4, -4, 16, 8, 8, -
NL: 22.0
WEIGHT: 32
DEGREE: 2
TERMS: 2
BALANCE: True
2 12

FOR X3
TT: |
0010000011010111011011011011100011001100110100001001100110111001
SEQUENCE:
 1 1 -1 1 1 1 1 1 -1 -1 1 -1 1 -1 -1 -1 1 -1 -1 1 -1 -1 1 -1 -1 1 -1 -1 -1 1 1
1 -1 -1 1 1 -1 -1 1 1 -1 -1 1 -1 1 1 1 1 -1 1 1 -1 -1 1 1 -1 -1 1 -1 -1 -1 1 1 -1
ANF:
0011000000000000000000000000000000000000000000000000000000000000
WHT:
0, 0, -8, -16, -12, -4, 4, 4, 8, 0, -8, 8, 12, -4, 4, 12, 8, 8, -8, 16, -4, 4, -12, -12, 8, -16, 0, 0, -4, -4, 12,
4, 0, 0, 8, 16, 4, -4, 4, 4, 8, 0, 8, 8, -4, -4, 4, 12, 0, 0, 16, -8, 4, -4, -4, -4, 16, -8, 8, -8, -12, 4, 4, -4
NL: 24.0
WEIGHT: 32
DEGREE: 2
TERMS: 2
BALANCE: True
2 12

FOR X4
TT:
0110110000110100110011101000110101010000000101001000111111011110
SEQUENCE:
 1 -1 -1 1 -1 -1 1 1 1 1 -1 -1 1 -1 1 1 -1 -1 1 1 -1 -1 -1 1 -1 1 1 1 -1 -1 1 -1 1
-1 1 -1 1 1 1 1 1 1 -1 1 -1 1 1 -1 1 1 1 -1 -1 -1 -1 -1 -1 1 -1 -1 -1 -1 -1 1
ANF:
0010000000000000000000000000000000000000000000000000000000000000
WHT:
0, 0, -8, 0, 8, 0, 16, 0, 0, 8, -8, 8, 0, 16, -8, 0, 16, 8, 8, 8, -16, 0, 8, 16, 0, 0, -8, 0, -8, 0, 0, 0, 0, 0,
-16, 8, 0, -8, 0, 0, -8, -16, -8, 8, 0, 0, 0, 8, -8, 0, 8, 8, 0, 0, 16, -8, 0, 0, 0, -8, 16, -8, 0, 16
NL: 24.0
WEIGHT: 32
DEGREE: 1
TERMS: 1
BALANCE: True
2
```

Fig 9. Screenshot of S-box 1 for calculating the non-linear values.

5. Time and Memory Required for Implementation

Python was used to implement the code. We utilized 512 GB SSD ROM and 16 GB RAM for simulation. Table 1 and Figure 10 display the amount of RAM needed to implement audio files as well as the associated graphical representation. The memory and time requirements for dynamic S-boxes are comparably lower than those for static S-boxes since S-boxes don't have to be saved anywhere and because they depend on the key[36][37].

Table 1. Memory Required for implementation in Static and Dynamic DES in Audio files

Memory (in KB)	***When the key is fixed***	***When there is 1 bit change in key***	***When there is 2 bit change in key***
Static DES	1736.778	1736.778	1736.778
Dynamic DES	626.819	626.819	626.819

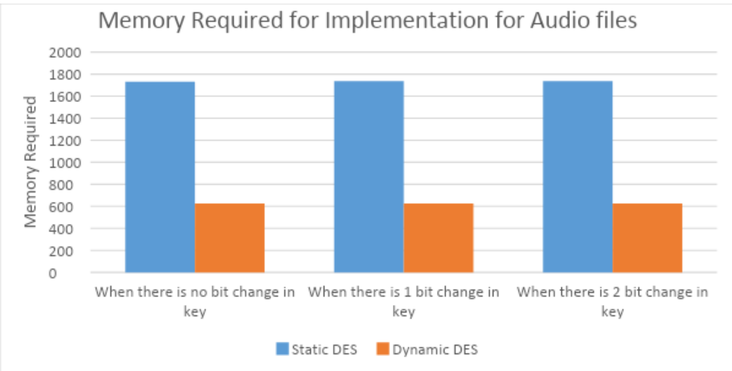

Fig 10. Comparison of memory required for Static and Dynamic DES in Video files.

The time required for implementation of audio files is given in the table 2 and this corresponding comparison of the time required in Static and Dynamic DES is shown in Figure 11[38].

Table 2. Time needed for implementation for Static and Dynamic DES in audio files.

Time (in sec)	***When the key is fixed***	***When there is 1 bit change in key***	***When there is 2 bit change in key***
Static DES	87.745	25.970	96.1685
Dynamic DES	73.648	25.3310	79.677

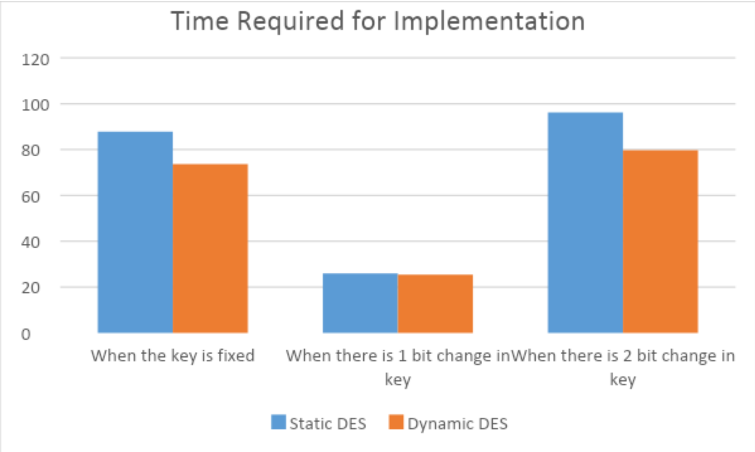

Fig 11. Comparison of time needed for Static and Dynamic DES in audio files.

Similarly, we can prove that the memory requirements as well as the time required for implementation is smallest for Dynamic DES compared with Static DES for video files also. Thus it is shown that in all the cases, the time and memory needed for Dynamic DES is less than Static DES both in audio and video files[39].

6. Robustness of linear cryptanalysis

Private-key block ciphers can be successfully attacked through differential and linear cryptanalysis techniques(Altaleb et al., 2017). The greatest entry in the Linear Approximation Table (LAT) determines how sophisticated is a linear cryptanalysis. The higher the values, the more susceptible the cipher is to cryptanalytic attacks. Linear approximation tables have been used to explain the robustness of linear cryptanalysis. By analyzing the Linear Approximation Table (LAT), one can determine the level of complexity involved in linear cryptanalysis. The existence of a vulnerable row in the S-box for linear cryptanalysis can be inferred from a high value in the LAT. The LAT for static and dynamic DES are displayed in Tables 3 and 4, respectively.

Table 3. LAT-static DES

a	**b**															
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	**16**	**8**	**8**	**8**	**8**	**8**	**8**	**8**	**8**	**8**	**8**	**8**	**8**	**8**	**8**	**8**
1	**8**	**8**	**6**	**6**	**8**	**8**	**6**	**14**	**10**	**10**	**8**	**8**	**10**	**10**	**8**	**8**
2	**8**	**8**	**6**	**6**	**8**	**8**	**6**	**6**	**8**	**8**	**10**	**10**	**8**	**8**	**2**	**10**
3	**8**	**8**	**8**	**8**	**8**	**8**	**8**	**8**	**10**	**2**	**6**	**6**	**10**	**10**	**6**	**6**
4	**8**	**10**	**8**	**6**	**4**	**4**	**6**	**8**	**8**	**6**	**10**	**10**	**10**	**4**	**10**	**8**
5	**8**	**6**	**6**	**8**	**8**	**8**	**12**	**10**	**6**	**8**	**10**	**10**	**8**	**6**	**6**	**8**
6	**8**	**10**	**6**	**12**	**8**	**8**	**8**	**10**	**8**	**6**	**12**	**12**	**6**	**8**	**8**	**6**

7	**8**	**6**	**8**	**10**	**4**	**4**	**10**	**8**	**6**	**8**	**8**	**8**	**12**	**10**	**8**	**10**
8	**8**	**8**	**8**	**8**	**8**	**8**	**8**	**8**	**6**	**10**	**6**	**6**	**10**	**6**	**6**	**2**
9	**8**	**8**	**6**	**6**	**8**	**8**	**6**	**6**	**4**	**8**	**10**	**10**	**8**	**12**	**10**	**6**
A	**8**	**12**	**6**	**10**	**8**	**8**	**10**	**6**	**10**	**10**	**8**	**8**	**10**	**10**	**8**	**8**
B	**8**	**12**	**8**	**4**	**8**	**8**	**12**	**8**	**8**	**8**	**8**	**8**	**8**	**8**	**8**	**8**
C	**8**	**6**	**12**	**6**	**8**	**8**	**10**	**8**	**10**	**8**	**12**	**12**	**8**	**10**	**8**	**6**
D	**8**	**10**	**10**	**8**	**12**	**12**	**8**	**10**	**4**	**6**	**8**	**8**	**10**	**8**	**8**	**10**
E	**8**	**10**	**10**	**8**	**4**	**4**	**8**	**10**	**6**	**8**	**6**	**6**	**4**	**10**	**6**	**8**
F	**8**	**6**	**4**	**6**	**8**	**8**	**10**	**8**	**8**	**6**	**6**	**6**	**6**	**8**	**10**	**8**

By analyzing the dynamic and static S-boxes, it can be noticed that the dynamic one has a higher value of 12 as its maximum value, while the static S-box has a maximum value of 14. This means that the largest entry in the Linear Approximation Table (LAT) of Dynamic DES is 12, indicating that the complexity of linear cryptanalysis is relatively low.

Table 4. LAT-dynamic DES

a	**b**															
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	**16**	**8**	**8**	**8**	**8**	**8**	**8**	**8**	**8**	**8**	**8**	**8**	**8**	**8**	**8**	**8**
1	**8**	**6**	**8**	**6**	**6**	**10**	**6**	**8**	**8**	**6**	**10**	**6**	**6**	**8**	**6**	**4**
2	**8**	**8**	**6**	**6**	**10**	**6**	**4**	**8**	**8**	**8**	**10**	**10**	**6**	**10**	**4**	**8**
3	**8**	**12**	**10**	**8**	**4**	**8**	**6**	**12**	**8**	**10**	**10**	**8**	**6**	**8**	**6**	**6**
4	**8**	**6**	**8**	**8**	**8**	**8**	**6**	**8**	**10**	**8**	**8**	**6**	**10**	**4**	**4**	**6**
5	**8**	**10**	**10**	**8**	**8**	**8**	**8**	**6**	**4**	**10**	**10**	**12**	**8**	**4**	**4**	**4**
6	**8**	**8**	**10**	**10**	**8**	**8**	**8**	**10**	**8**	**6**	**6**	**10**	**6**	**8**	**12**	**8**
7	**8**	**8**	**6**	**4**	**10**	**8**	**10**	**4**	**6**	**10**	**8**	**10**	**12**	**6**	**6**	**8**
8	**8**	**6**	**4**	**4**	**4**	**12**	**10**	**10**	**6**	**6**	**8**	**8**	**10**	**8**	**10**	**10**
9	**8**	**12**	**6**	**6**	**2**	**8**	**6**	**6**	**4**	**8**	**8**	**6**	**8**	**8**	**10**	**10**
A	**8**	**4**	**6**	**4**	**6**	**8**	**6**	**12**	**10**	**8**	**10**	**8**	**10**	**8**	**2**	**10**
B	**8**	**10**	**6**	**8**	**10**	**6**	**8**	**10**	**8**	**10**	**8**	**10**	**8**	**8**	**10**	**8**
C	**8**	**4**	**4**	**8**	**6**	**10**	**12**	**12**	**10**	**4**	**8**	**8**	**8**	**10**	**10**	**6**
D	**8**	**6**	**10**	**6**	**6**	**6**	**8**	**6**	**4**	**6**	**8**	**6**	**10**	**10**	**6**	**6**
E	**8**	**8**	**12**	**8**	**8**	**10**	**6**	**6**	**6**	**10**	**8**	**8**	**4**	**8**	**10**	**10**
F	**8**	**2**	**8**	**6**	**6**	**8**	**8**	**8**	**8**	**8**	**8**	**10**	**6**	**6**	**6**	**12**

7. Robustness to Differential Cryptanalysis

Private-key block ciphers can be vulnerable to powerful cryptanalytic attacks called Differential Cryptanalysis. Differential cryptanalysis's effectiveness is determined by two elements: The highest number in the XOR table and the total number of 0's in the table. To execute this attack, a Differential Distribution Table (DDT) is used to record the differentials. Table 5 exhibits the DDT for static DES, while Table 6 displays the DDT for dynamic DES.

Table 5. DDT of static DES

a'	b'															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	2	0	0	0	2	0	2	4	0	4	2	0	0
2	0	0	0	2	0	6	2	2	0	2	0	0	0	0	2	0
3	0	0	2	0	2	0	0	0	0	4	2	0	2	0	0	4
4	0	0	0	2	0	0	6	0	0	2	0	4	2	0	0	0
5	0	4	0	0	0	2	2	0	0	0	4	0	2	0	0	2
6	0	0	0	4	0	4	0	0	0	0	0	0	2	2	2	2
7	0	0	2	2	2	0	2	0	0	2	2	0	0	0	0	4
8	0	0	0	0	0	0	2	2	0	0	0	4	0	4	2	2
9	0	2	0	0	2	0	0	4	2	0	2	2	2	0	0	0
A	0	2	2	0	0	0	0	0	6	0	0	2	0	0	4	0
B	0	0	8	0	0	2	0	2	0	0	0	0	0	2	0	2
C	0	2	0	0	2	2	2	0	0	0	0	2	0	6	0	0
D	0	4	0	0	0	0	0	4	2	0	2	0	2	0	2	0
E	0	0	2	4	2	0	0	0	6	0	0	0	0	0	2	0
F	0	2	0	0	6	0	0	0	0	4	0	2	0	0	2	0

Table 6. DDT of Dynamic DES

a'	b'															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	4	2	0	0	0	0	6	0	0	0	2	0	0	2	0
2	0	0	0	2	0	2	4	0	0	0	2	0	2	0	0	4
3	0	2	2	0	2	0	0	2	4	0	0	0	0	4	0	0
4	0	2	0	0	0	0	2	0	4	2	4	0	0	0	2	0
5	0	0	0	2	0	0	0	2	2	2	2	0	0	4	0	0
6	0	0	2	0	2	2	0	2	0	2	0	0	2	0	2	2
7	0	0	2	0	0	4	2	0	2	2	0	2	0	0	2	0
8	0	4	0	2	0	2	0	0	0	0	2	0	0	2	2	2
9	0	2	2	0	4	0	4	0	0	0	0	0	2	0	0	2
A	0	0	2	2	2	2	0	0	0	2	0	2	2	0	2	0
B	0	0	4	2	0	2	0	0	0	2	0	0	2	2	2	0
C	0	0	0	0	0	0	2	2	0	2	0	6	2	0	0	2
D	0	0	0	0	0	2	0	2	0	2	0	0	4	2	2	0
E	0	2	0	2	4	0	0	0	0	0	4	0	0	2	0	2
F	0	0	0	2	2	0	2	0	2	0	2	4	2	0	0	0

To enhance the S-box's resistance against differential cryptanalysis, it is advisable to have more non-zero entries. The Dynamic S-box has a higher number of non-zero entries in its Differential Distribution Table (DDT) compared to the static S-box, thereby making it even more resilient against differential cryptanalysis. Moreover, our

Dynamic S-box meets the requirement of having low propagation criteria while also maintaining a good XOR profile across its rows through minimal variations.Tables 7 and 8 provide a comparison of the performance metrics between the original and dynamic DES.In both tables T is denoted as true. Based on the aforementioned analysis, it is clear that the Dynamic S-box outperforms the static S-box in several areas including linearity, SAC, balance, robustness to both linear and differential cryptanalysis, and implementation time and memory requirements.

Table 7. Performance value of original Sbox DES

Sbox	Index	Nonlinearity	Balance	XOR Table	LAT
DES Sbox1	1	18	T	16	14
	2	22	T		
	3	20	T		
	4	18	T		
DES Sbox2	1	18	T	16	10
	2	18	T		
	3	20	T		
	4	22	T		
DES Sbox3	1	21.5	T	16	16
	2	18.5	T		
	3	22.5	T		
	4	21.5	T		
DES Sbox4	1	22	T	16	16
	2	22	T		
	3	22	T		
	4	22	T		
DES Sbox5	1	20	T	16	14
	2	18	T		
	3	20	T		
	4	22	T		
DES Sbox6	1	20	T	16	14
	2	20	T		
	3	20	T		
	4	20	T		
DES Sbox7	1	20	T	16	14
	2	14	T		
	3	22	T		
	4	18	T		
DES Sbox8	1	22	T	16	16
	2	20	T		
	3	20	T		
	4	22	T		

Table 8. Performance value of dynamic S-box DES

Sbox	Index	Nonlinearity	Balance	XOR Table	LAT
DES Sbox1	1	22	T	16	12
	2	22	T		
	3	24	T		
	4	24	T		
DES Sbox2	1	22	T	16	10
	2	22	T		
	3	22	T		
	4	20	T		
DES Sbox3	1	20	T	14	12
	2	20	T		
	3	22	T		
	4	22	T		
DES Sbox4	1	22	T	16	14
	2	22	T		
	3	22	T		
	4	22	T		
DES Sbox5	1	22	T	16	14
	2	18	T		
	3	22	T		
	4	22	T		
DES Sbox6	1	22	T	14	14
	2	16	T		
	3	22	T		
	4	24	T		
DES Sbox7	1	20	T	16	14
	2	20	T		
	3	22	T		
	4	22	T		
DES Sbox8	1	22	T	16	16
	2	22	T		
	3	24	T		
	4	24	T		

8. Conclusion

As previously stated, security is an essential element in all aspects of modern society, and the primary aim of digital data exchange is to safeguard data against various threats, raising the security level to the next level. In this study, we have presented an effective method for creating a multi-functional S-box using dynamic DES to protect audio and video files' digital data against a variety of attacks. The utilization of diverse function generation distributed among 8 S-boxes has made it impossible for attackers to even approximate the probability, as the level of protection has been raised significantly. As previously stated, security is a crucial factor in today's society across all fields. Currently, the primary goal of transmitting digital data is to enhance security measures and provide protection against various risks.

Table 9. Abbreviations

AES	Advance Encryption Standard
DES	Data Encryption Standard
DDT	Differential Distribution Table
LAT	Linear Approximation Table
RSA	Rivest–Shamir–Adleman
SCTT	Simple Column Transposition Technique
VMS	Variable Mapping S-box
GA	Genetic Algorithm
LFSR	Linear Feedback Shift Register
PN	Pseudorandom Generator
SAC	Strict Avalanche Criterion
SNR	Signal to Noise Ratio
DPA	Differential Power Analysis

References

[1] Hellman, Martin E. "I.des will be totally insecure within ten years'." IEEE spectrum 16.7 (1979): 32-40.

[2] Alani, Mohammed M. "DES96-improved DES security." 2010 7th International Multi-Conference on Systems, Signals and Devices. IEEE, 2010.

[3] Manikandan, G., et al. "A modified crypto scheme for enhancing data security." Journal of Theoretical and applied information Technology 35.2 (2012): 149-154.

[4] Shah Kruti, R., and Bhavika Gambhava. "New approach of data encryption standard algorithm." International Journal of Soft Computing and Engineering (IJSCE) ISSN (2012): 2231-2307.

[5] Arya, Govind Prasad, et al. "A cipher design with automatic key generation using the combination of substitution and transposition techniques and basic arithmetic and logic operations." The SIJ Transactions on Computer Science Engineering & its Applications (CSEA) 1.1 (2013): 21-24.

[6] Wong, Duncan S., Hector Ho Fuentes, and Agnes Hui Chan. "The performance measurement of cryptographic primitives on palm devices." Seventeenth Annual Computer Security Applications Conference. IEEE, 2001.

[7] Rivest, Ronald L., Adi Shamir, and Leonard Adleman. "A method for obtaining digital signatures and public-key cryptosystems." Communications of the ACM 21.2 (1978): 120-126.

[8] Juremi, Julia, Ramlan Mahmod, and Salasiah Sulaiman. "A proposal for improving AES S-box with rotation and key-dependent." Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec). IEEE, 2012.

[9] Al-Muhammed, Muhammed Jassem. "Light but Effective Encryption Technique based on Dynamic Substitution and Effective Masking." International Journal of Advanced Computer Science and Applications 9 (2018).

[10] Singh, Sombir, Sunil K. Maakar, and Dr Sudesh Kumar. "Enhancing the security of DES algorithm using transposition cryptography techniques." International Journal of Advanced Research in Computer Science and Software Engineering 3.6 (2013): 464-471.

[11] Gupta, Nimmi. "Implementation of optimized des encryption algorithm upto 4 round on spartan 3." International Journal of Computer Technology and Electronics Engineering (IJCTEE) 2.1 (2012): 82-86.

[12] Patel, Payal, Kruti Shah, and Khushbu Shah. "Enhancement Of Des Algorithm With Multi State Logic." International Journal of Research in Computer Science 4.3 (2014): 13.

[13] Albassalli, A. M. B., and A-MA Wahdan. "Genetic algorithm cryptanalysis of a feistel type block cipher." International Conference on Electrical, Electronic and Computer Engineering, 2004. ICEEC'04.. IEEE, 2004.

[14] Sharma, Arvind Kumar, and Hitesh Sharma. "New Approach To Des With Enhanced Key Management And Encryption/Decryption System (Des Ultimate)." International Journal of Advances in Engineering & Technology 8.3 (2015): 368.

[15] Krishnamurthy, G. N., and V. Ramaswamy. "Making AES stronger: AES with key dependent S-box." IJCSNS International Journal of Computer Science and Network Security 8.9 (2008): 388-398.

[16] Mahmoud, Eman Mohammed, et al. "Enhancing channel coding using AES block cipher." International Journal of Computer Applications 61.6 (2013).

[17] Zahid, Amjad Hussain, Eesa Al-Solami, and Musheer Ahmad. "A novel modular approach-based substitution-box design for image encryption." IEEE Access 8 (2020): 150326-150340.

[18] Patil, S. D. ., & Deore, P. J. . (2023). Machine Learning Approach for Comparative Analysis of De-Noising Techniques in Ultrasound Images of Ovarian Tumors. International Journal on Recent and Innovation Trends in Computing and Communication, 11(2s), 230–236. https://doi.org/10.17762/ijritcc.v11i2s.6087

[19] Oukili, Soufiane, and Seddik Bri. "High speed efficient advanced encryption standard implementation." 2017 International Symposium on Networks, Computers and Communications (ISNCC). IEEE, 2017.

[20] Alabaichi, Ashwak, and Adnan Ibrahem Salih. "Enhance security of advance encryption standard algorithm based on key-dependent S-box." 2015 Fifth International Conference on Digital Information Processing and Communications (ICDIPC). IEEE, 2015.

[21] Altaleb, Anas, et al. "An algorithm for the construction of substitution box for block ciphers based on projective general linear group." AIP Advances 7.3 (2017): 035116.

[22] Anees, Amir, and Zeeshan Ahmed. "A technique for designing substitution box based on van der pol oscillator." Wireless Personal Communications 82.3 (2015): 1497-1503.

[23] Akande, Oluwatobi Noah, et al. "A Dynamic Round Triple Data Encryption Standard Cryptographic Technique for Data Security." International Conference on Computational Science and Its Applications. Springer, Cham, 2020.

[24] Ullah, Atta, Sajjad Shaukat Jamal, and Tariq Shah. "A novel scheme for image encryption using substitution box and chaotic system." Nonlinear Dynamics 91.1 (2018): 359-370.

[25] Siddiqui, Nasir, et al. "A Novel Algebraic Technique for Design of Computational Substitution-Boxes Using Action of Matrices on Galois Field." IEEE Access 8 (2020): 197630-197643.

[26] Khan, Fadia Ali, et al. "A new technique for designing 8× 8 substitution box for image encryption applications." 2017 9th Computer Science and Electronic Engineering (CEEC). IEEE, 2017.

[27] Nilima, S., and Arora Nitin. "Randamization Technique for Desiging of Substitution Box in Data Encryption Standard Algorithm." International Journal of Mathematical Sciences and Computing 5.3 (2019): 27-36.

[28] Adhie, Roy Pramono, et al. "Implementation cryptography data encryption standard (DES) and triple data encryption standard (3DES) method in communication system based near field communication (NFC)." Journal of Physics: Conference Series. Vol. 954. No. 1. IOP Publishing, 2018.

[29] Akhtar, Tanveer, Nizamud Din, and Jamal Uddin. "Substitution box design based on chaotic maps and cuckoo search algorithm." 2019 International conference on advanced communication technologies and networking (CommNet). IEEE, 2019.

[30] Dr. Bhushan Bandre. (2013). Design and Analysis of Low Power Energy Efficient Braun Multiplier. International Journal of New Practices in Management and Engineering, 2(01), 08 - 16. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/12

[31] Khan, Fadia Ali, et al. "A novel substitution box for encryption based on Lorenz equations." 2017 International Conference on Circuits, System and Simulation (ICCSS). IEEE, 2017.

[32] Arshad, Sadiqa, and Majid Khan. "New extension of data encryption standard over 128-bit key for digital images." Neural Computing and Applications (2021): 1-14.

[33] Siddiqui, Nasir, et al. "A highly nonlinear substitution-box (S-box) design using action of modular group on a projective line over a finite field." Plos one 15.11 (2020): e0241890.

[34] Khan, Muhammad Fahad, Adeel Ahmed, and Khalid Saleem. "A novel cryptographic substitution box

design using Gaussian distribution." IEEE Access 7 (2019): 15999-16007.

[35] Mr. Rahul Sharma. (2013). Modified Golomb-Rice Algorithm for Color Image Compression. International Journal of New Practices in Management and Engineering, 2(01), 17 - 21. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/13

[36] Riaz, Fozia, and Nasir Siddiqui. "Design of an Efficient Cryptographic Substitution Box by using Improved Chaotic Range with the Golden Ratio." International Journal of Computer Science and Information Security (IJCSIS) 18.1 (2020).

[37] Rahaman, Ziaur, et al. "A novel structure of advance encryption standard with 3-dimensional dynamic S-Box and key generation matrix." arXiv preprint arXiv:2005.00157 (2020).

[38] Alghafis, Abdullah, Noor Munir, and Majid Khan. "An encryption scheme based on chaotic Rabinovich-Fabrikant system and S 8 confusion component." Multimedia Tools and Applications 80.5 (2021): 7967-7985.

[39] Ahmad, Musheer, et al. "Particle swarm optimization based highly nonlinear substitution-boxes generation for security applications." IEEE Access 8 (2020): 116132-116147.

[40] Seghier, Athmane, Jianxin Li, and Da Zhi Sun. "Advanced encryption standard based on key dependent S-Box cube." IET Information Security 13.6 (2019): 552-558.

[41] Akande, Oluwatobi Noah, et al. "A Dynamic Round Triple Data Encryption Standard Cryptographic Technique for Data Security." International Conference on Computational Science and Its Applications. Springer, Cham, 2020.

[42] Özkaynak, Fatih, and Mukhlis I. Muhamad. "Alternative substitutional box structures for DES." 2018 6th International Symposium on Digital Forensic and Security (ISDFS). IEEE, 2018