iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

BINARY STREAM SCATTERING (BSS) METHOD TO PROTECT DSF

Khawla Tawfeeq Rasheed Omar,
Rose Mufid Abd Alraheem Alqasem,
Samah AbdulMohdi Abdallah Massadeh,
Samer Abdullah Sadeq Hamed,
Nawal Ameen Ahmed Alzabin,
Al-Balqa Applied University Jordan-Amman

ABSTRACT
In today's interconnected digital world, the transmission of digital speech files is ubiquitous across diverse communication platforms. With the proliferation of sensitive and specialized information being exchanged, safeguarding these messages from potential threats such as intruders, abusers, and data hackers becomes imperative. This research paper introduces an innovative approach aimed at streamlining digital speech signal protection procedures while concurrently thwarting hacking attempts. At the core of this method lies the utilization of a sophisticated variable content private key designed to facilitate ease of alteration without compromising the integrity of encryption and decryption operations. The pivotal aspect involves leveraging a chaotic logistic map model to generate the required indices keys, scattering the speech stream of bits and scattering back these blocks. The presented method will be simple, it will use simple chaotic logistic map model to generate the required secret indices key, simple bits scattering to apply speech file encryption and simple scattering back operation to apply speech decryption.
The presented method will be flexible, it will provide the user with the ability to change the number of rounds, the block size and the private key length, making these changes will not affect the encryption and decryption function.
The presented method will be highly secure, it will use a 576 bits private key, and this length will be increased when increasing the number of used rounds.
The presented method will provide a high speed, it will reduce both the encryption and decryption times and it will provide a good speed up comparing with other existing methods of data cryptography.
The presented method is empirically validated through the implementation of various digital speech files. Comparative analyses against existing methods underscore the efficacy and robustness of the presented method, substantiating its significant advancements in data protection paradigms.

Keywords:
DSF, cryptography, PK, SIK, CS, CLMM, SBM, SBS, block.

INTRODUCTION

Digital speech file (DSF) [1-10] is a collection of samples values arrange in one column matrix (mono speech) or in two columns matrix (stereo speech), each sample represents the amplitude of the sample, and this value is a double fractional value within the range -1 to +1. DSF can be represented by the wave plot, histogram (see figure 1) [11-15]. The samples values can be converted to binary to form the speech binary matrix (SBM), and this matrix can be reshaped to one row matrix to form the speech binary stream (SBS) (see figure 1) [16-20[.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

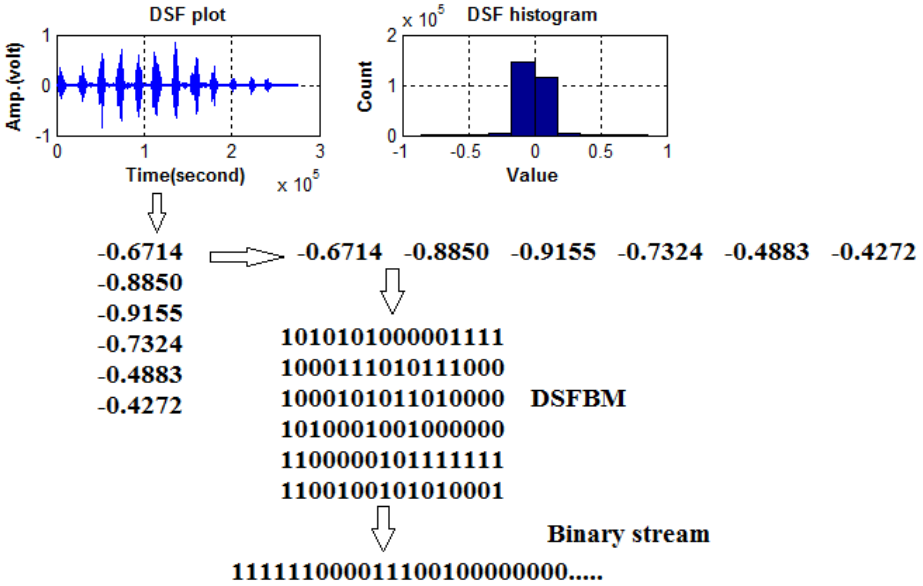

Figure 1: DSF presentation

DSF is usually used to create the voiceprint, and this print has the following features [21-30]:

- Voice recognition doesn't require specialized devices to capture biometric data like fingerprints or iris scans; a phone speaker or the microphone included with computers can do the job.
- Voice recognition has solved the problem of theft and forgery of passwords and cards.
- Voice recognition allows for remote identification and verification.
- Voice recognition has helped people avoid memorizing passwords.
- . Voice recognition is limited to living individuals.
- Voice recognition has expedited the identity verification process, as voice recognition-based applications don't require an employee presence.
- Voice recognition is a good alternative for people who have difficulty using a mouse or keyboard.
- Voice recognition is a secure way to track a user's activity and verify that they are the authorized user, unlike passwords which grant full access to any system once the user knows the password.

Voiceprint is used in many applications, including [31-35]:

- Identifying suspects in crimes and security cases.
- Accessing databases such as passports, university and school records, medical records, and employee records.
- Accessing financial transactions, such as those conducted by banks, commercial markets, and travel and tourism agencies.
- Accessing physical locations, such as homes, offices, and vehicles.
- Using devices such as computers, cameras, home appliances, and elevators.

With the increasing reliance on digital communication, securing voice and video calls has become crucial. Modern applications rely on advanced encryption technologies to protect data in transit, preventing unauthorized parties from intercepting conversations. In this article, we'll discuss how encryption works in communication applications, the importance of using it, and best practices to ensure the security of your digital calls [36-40].

In the digital age, video and voice calls have become commonplace, both personally and professionally. However, this development has been accompanied by growing security threats, as hackers or unauthorized entities can intercept or eavesdrop on conversations. For this reason, encryption has become a fundamental technology for protecting user privacy and preventing any potential breaches [41-45].

In fact, most modern applications rely on strong encryption to ensure call security. But how does this encryption work? And do all applications offer the same level of protection? In this article, we'll explore how encryption works, how to ensure your calls are protected, and some of the challenges these technologies may face [46-50].

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

The importance of voice encryption lies in protecting the privacy of voice communications and their data by converting them into an unreadable format, thus preventing unauthorized access. Encryption also contributes to reducing the size of audio files and facilitating their storage and transfer, while preserving the original sound quality and ensuring data integrity and preventing tampering [51-55].
Without a doubt, encryption is one of the most effective ways to protect data while it is transmitted over the internet. It helps to [56-60]:

- Protect privacy: Prevention of Eavesdropping: Encryption protects against eavesdropping on calls and voice communications, as signals are encoded so that they can only be understood by authorized parties using the correct encryption key, Encryption provides a barrier against hackers and intruders, preventing data theft or misuse, even if networks or devices are compromised.
- Combat electronic eavesdropping: Reduce the chances of communications being intercepted or data being intercepted by hackers.
- Comply with security regulations: Laws such as GDPR and HIPAA require companies to use strong encryption technologies to protect data.
- Ensure the confidentiality of sensitive information: Call encryption is essential for companies that handle sensitive data, such as financial institutions or government sectors.

DSF crypto method as shown in figure 2 usually contains two parts [61-66]: the sending (encrypting) part and the receiving (decrypting) part. The encrypting part uses the encryption function (EF) to process the source DSF and the private key (PK) to produce an encrypted (cipher) DSF, while the receiving part uses the decryption function (DF) to process the encrypted DSF and the PK to produce a decrypted DSF.
The method of DSF cryptography will be classified as a good method it meets the following requirements:

- Encryption quality: The encrypted DSF must be damaged, corrupted and unlistenable, the quality parameters values measured between the source and the encrypted DSFs must be as follows [67-70]:
  - High value of MSE (mean square error).
  - Low value of PSNR (peak signal to noise ratio).
  - Low value of CC (correlation coefficient).
- Encryption quality: The decrypted DSF must be the same as the source one, the quality parameters values measured between the source and the decrypted DSFs must be as follows [71-76]:

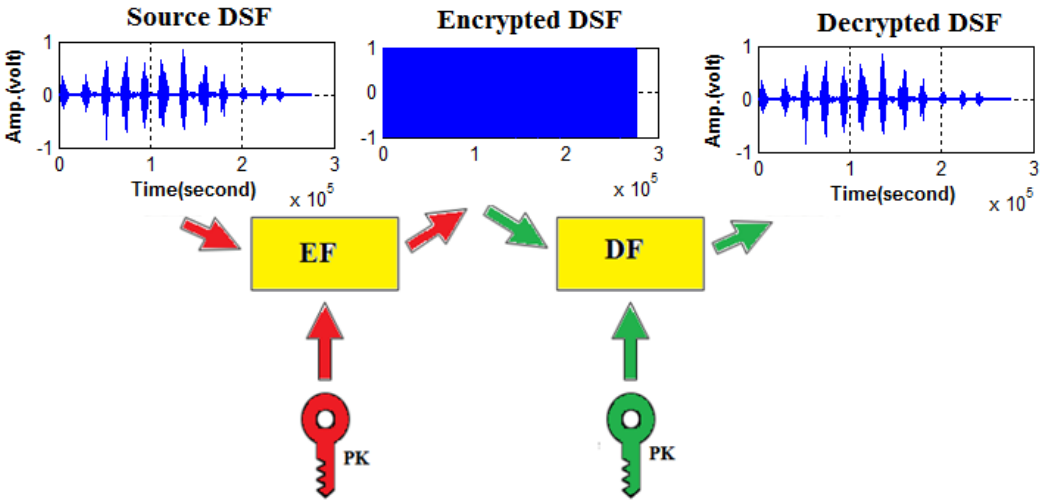

Figure 2: DSF crypto method diagram

  - Zero MSE.
  - Infinite PSNR).
  - CC must equal 1.
- Speed: The method must optimize the speed of DSF cryptography by reducing both of the encryption and decryption times [77-81].
- Level of security: The method must use a complicated PK, the PK length must be greater than 100 bits, this length will be strong and it will provide a key space capable to resist hacking attacks, the decrypted DSF must be sensitive to the selected PK [82-86].

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

- Simplicity: The method must use simple procedures for key generation, DSF encryption and DSF decryption.
- Flexibility: The method must provide the user with the ability to change the number of rounds, the block size and the PK length, making any of these changes must not affect the EF and the DF.

RELATED WORKS

Multiple and varied methods for data encryption are now available, and many of these methods rely on standard approaches such as des (data encryption standard), AES (advanced encryption standard) and BF (blowfish) methods [1-5].

Standard methods share many characteristics, and some of these characteristics need improvement, which will be provided by the method proposed in this research. Among these characteristics, we mention the following [6-10]:

- Data size: Standard methods handle small datasets efficiently, such as confidential messages, but increasing the size of the data to be encrypted reduces the efficiency of these methods. The presented BSS method will be efficiently used to encrypt-decrypt data with big size such as DSF.
- Rounds: Standard method are to be implemented in a number of rounds with the following features:
  - The number of rounds is fixed and cannot be changed by the user.
  - All rounds must be executed.
  - Rounds are dependent, and all rounds are used to treat the same data block.

  The presented method will use a variable number of rounds, this number will be selected by the user and the rounds will be independent.
- Data blocking: Standard methods divide the data into blocks with the following features:
  - Block size in bits is small.
  - Block size is fixed and cannot be changed by the user.
  - All rounds use the same block size.

  The presented method will use a variable block size, each round will use its own block size, the block size can be small or big and it will be selected by the user.
- PK length: Standard methods use a fixed length PK, it cannot be changed and it is varies from short PK length to long PK key length. The presented BSS method will use a variable length PK, and it will use 192 bits length for each selected round.
- Security level: The security level depends on the length of the used PK, figure 3 shows the key space provided by the presented method, and comparing with standard method the BSS method will increase the security level by providing a huge key space.
- Speed: Standard methods provide a low speed of data cryptography especially when they are used to encrypt-decrypt big data such as DSF. Some authors introduced some chaotic methods to enhance the performance of standard method and they succeeded [1-5]. The presented BSS method will enhance the speed of DSF cryptography and it will provide a good speed up comparing with standard methods.

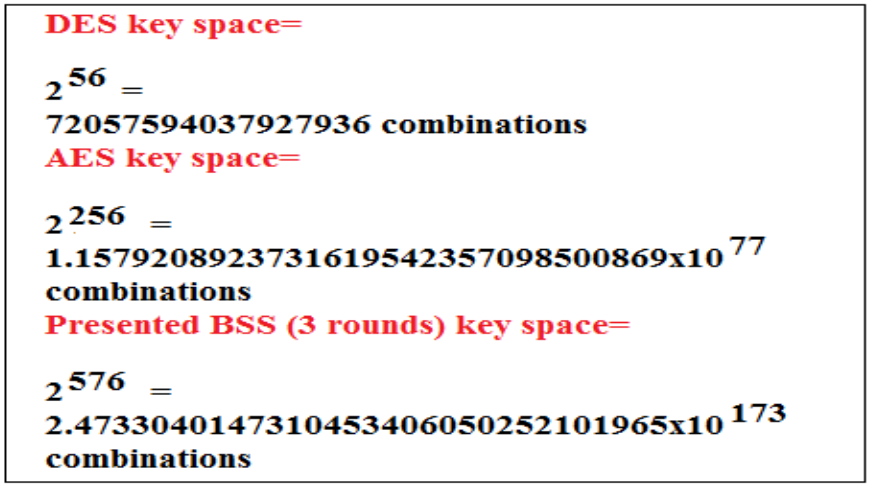

Figure 3: Provided key spaces of various methods

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

- Simplicity: Standard methods are not simple, they use a complicated sequence of operations to generate the secret keys, encrypt and decrypt the data.
- Flexibility: Standard methods are not flexible, the number of rounds, the PK length and the block size are fixed, and the user cannot change any of these parameters. The presented method will provide the user with the ability to change the number of rounds, the block size and the PK length, and making these changes will not affect the EF and DF.
-

METHODOLOGY

The presented in this paper research BSS is a variable number of rounds method, and it can be implemented at least with one round. The rounds are independent and each round uses it PK part and the input DSF to encrypt-decrypt the input DSF as shown in figure 4.

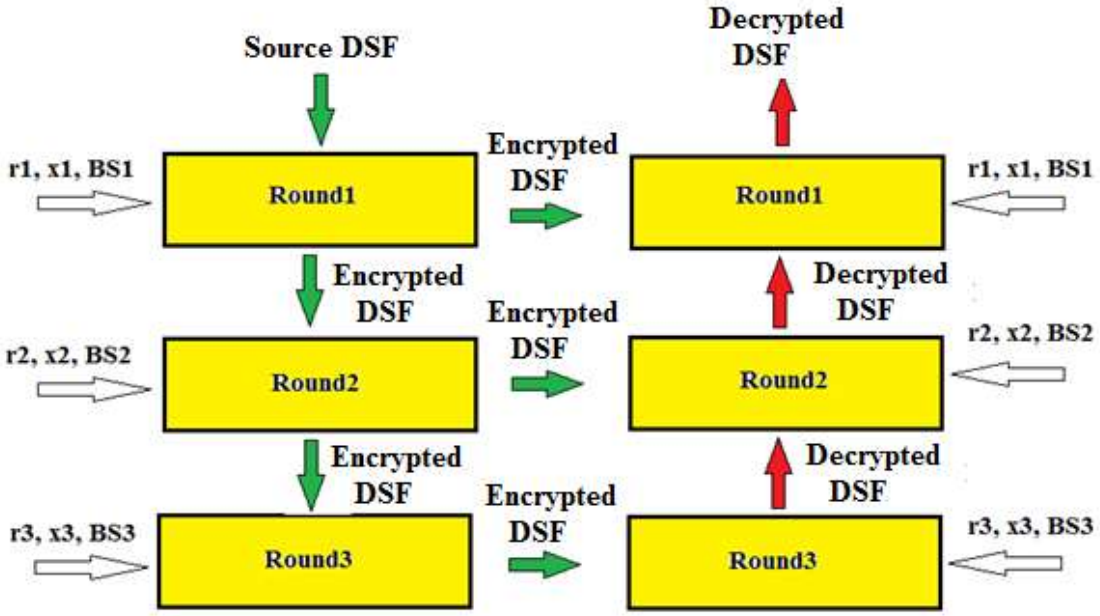

Figure 4: Presented BSS method with three rounds diagram

The block size value in the PK (BS) is to be used to calculate the number of blocks in the associated round, while the values of the chaotic logistic parameters r and x are to be used to run a chaotic logistic map model to generate a chaotic sequence, this sequence will be sorted to form the secret indices key, which will be used to scatter/scatter back the DSF blocks of bits in the encryption/decryption process.
Generating the secret indices key is a simple process, and figure 5 shows an example of running a CLMM to generate the SIK.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

```
NB=8;
r=3.77;x=0.12;
for i=1:NB
CS(i)=x;
x=x*r*(1-x);
end
[css SIK]=sort(CS);
```

```
CS =
   0.1200   0.3981   0.9034   0.3291   0.8324   0.5259   0.9400   0.2127
SIK =
   1   8   4   2   6   5   3   7
```

Figure 5: Example of generating SIK

The generated SIK will be very sensitive any minor changes in r, x, and NB will lead to generate a new SIK, so the encryption and decryption parts must use the same PK.
Each round in the encryption/decryption part will be used to implement the following tasks:

a) Converting the DSF to a binary stream, and this can be done bt performing the following operations:
- Convert the DSF to binary to get the speech binary matrix (SBM).
- Reshape the 16 columns SBM to one row matrix to get the speech binary stream (SBS).

b) Calculate the number of blocks (NB) by dividing the length of BS by the value of BS.
c) Use the values of r, x and NB to generate the chaotic sequence (CS) by running a CLMM.
d) Sort the CS to get the SIK.
e) Use SIK to scatter/scatter back the SBS blocks to encrypt/decrypt the DSF.
f) Reshape SBS back to SBN.
g) Convert SBM to decimal to get the encrypted/decrypted DSF.

The SBS scattering is a simple task, and it will be implemented based on the contents of the generated SIK by applying the following:
For each output block with index i, replace this block by the input block with index c, where c is the contents of SIK with index i (see figures 6 and 8).
The SBS scattering back is a simple task, and it will be implemented based on the contents of the generated SIK by applying the following:
For each output block with index c, replace this block by the input block with index i, where c is the contents of SIK with index i (see figures 7 and 9).

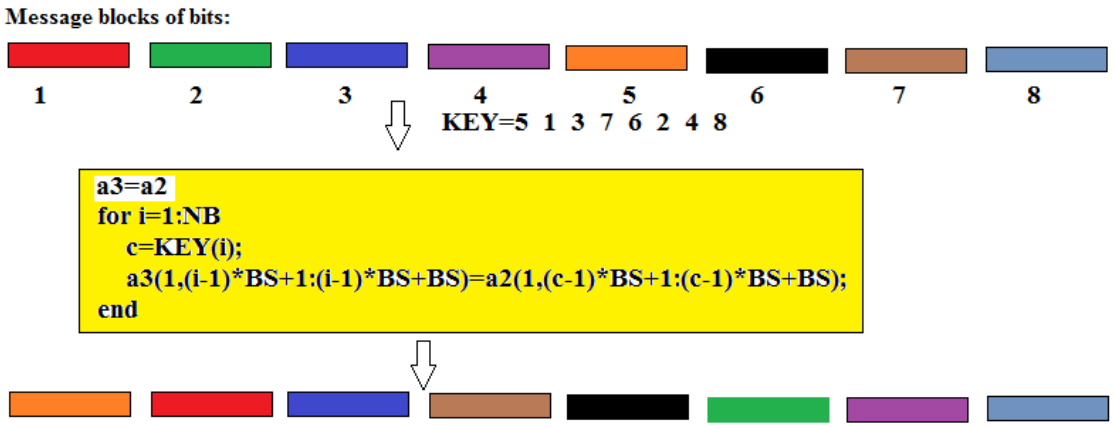

Figure 6: Scattering operation example

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

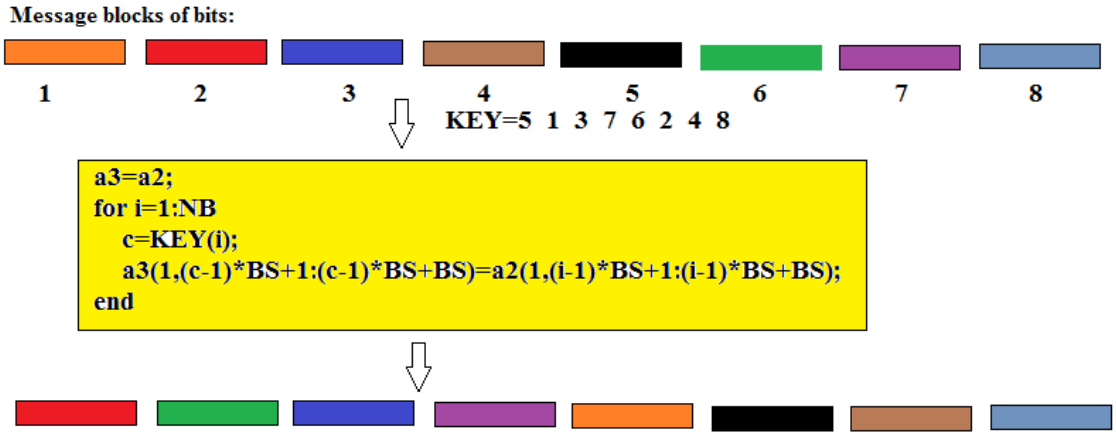

Figure 7: Scattering back operation example

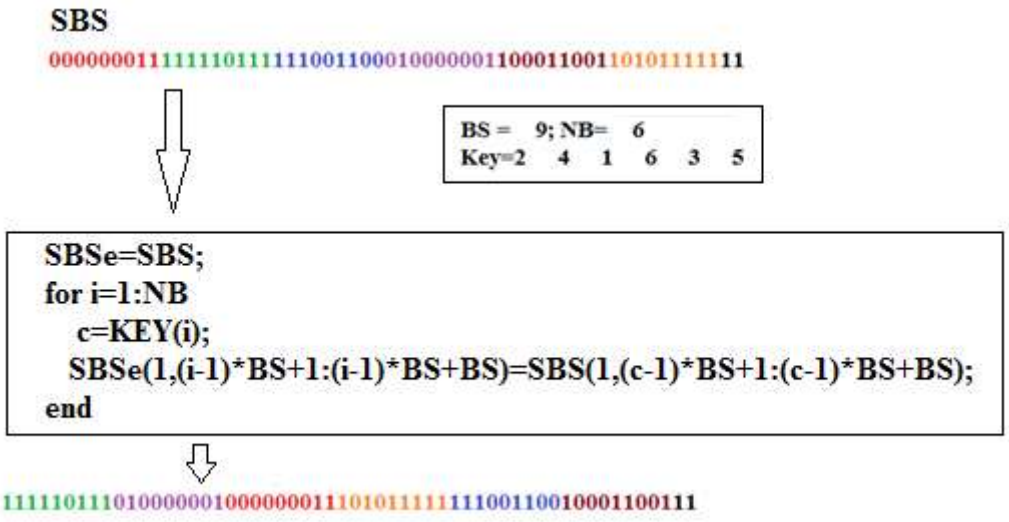

Figure 8: DSF encryption example

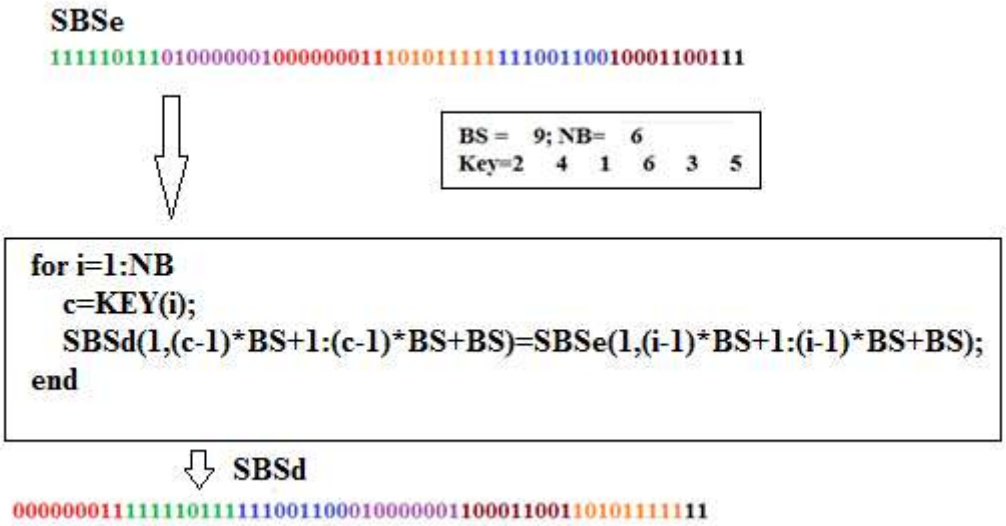

Figure 9: DSF decryption example

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

Each encryption-decryption round will be implemented by calling the EF/DF shown in figure 10 and 11:

```
function [spe]=BITS_ENC(sp,BS,r,x)
q1 = quantizer('fixed');
[n1 n2]=size(sp);S1=n1*n2;
a=reshape(sp,1,S1);
a1=num2bin(q1,a);
NB=fix(S1*16/BS);
for i=1:NB
   x=x*r*(1-x);
   CLDS(i)=x;
end
[rr KEY]=sort(CLDS);
a2=reshape(a1,1,S1*16);
a3=a2;
for i=1:NB
   c=KEY(i);
   a3(1,(i-1)*BS+1:(i-1)*BS+BS)=a2(1,(c-1)*BS+1:(c-1)*BS+BS);
end
a33=reshape(a3,S1,16);
spe1=bin2num(q1,a33)';
spe=reshape(spe1,n1,n2);
end
```

Figure 10: Presented BSS EF

```
function [spd]=BITS_DEC(sp,BS,r,x)
q1 = quantizer('fixed');
[n1 n2]=size(sp);S1=n1*n2;
a=reshape(sp,1,S1);
a1=num2bin(q1,a);
NB=fix(S1*16/BS);
for i=1:NB
   x=x*r*(1-x);
   CLDS(i)=x;
end
[rr KEY]=sort(CLDS);
a2=reshape(a1,1,S1*16);
a3=a2;
for i=1:NB
   c=KEY(i);
   a3(1,(c-1)*BS+1:(c-1)*BS+BS)=a2(1,(i-1)*BS+1:(i-1)*BS+BS);
end
a33=reshape(a3,S1,16);
spe1=bin2num(q1,a33)';
spd=reshape(spe1,n1,n2);
end
```

Figure 11: Presented BSS DF

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

RESULTS

The proposed BSS method was implemented using MATLAB 7, capitalizing on the computational capabilities of a processor operating at 2.4 MHz and an Intel i5 processor with a RAM capacity of 8 GB.

Encryption and decryption times are among the most important factors used in evaluating the performance of an encryption method, especially when dealing with large amounts of data such as DSF.

DSF encryption with the original standard algorithms is time-consuming and generally considered too slow for modern applications. For example, encrypting a 500KB DSF took DES 476 seconds, whereas chaotic algorithms took only 14 seconds on the same system. While DES can encrypt 1KB of DSF in under a millisecond (around 0.00099 seconds), DSF data is significantly larger, and the total time depends heavily on image size and system hardware and the following factors affect the DSF encryption-decryption time:

- DSF size**:** The larger the DSF, the longer it will take to encrypt.
- Hardware and software**:** The speed of the computer's CPU and the software used for encryption (e.g., MATLAB) will impact the final encryption time.
- Algorithm efficiency**:** Modern algorithms can achieve faster encryption speeds compared to the original DES algorithm, especially for DSFs. Some research shows that algorithms with a different architecture, such as those using chaotic systems, are significantly faster for DSF encryption.

To test the speed of the presented BSS method various DSF were selected and implemented using the presented BSS method, the encryption time (ET) and the decryption time (DT) were calculate and table 1 shows the obtained speed results:

Table 1: BSS method speed results (one round)

DSF size (K bytes)	ET	DT
10	0.0900	0.0330
12	0.0920	0.0330
15	0.0990	0.0350
18	0.1060	0.0370
20	0.1100	0.0410
25	0.1170	0.0510
30	0.1290	0.0600
40	0.1700	0.0850
50	0.2210	0.1470
75	0.2260	0.1480
100	0.2680	0.2000
200	0.4710	0.3890
500	1.0710	1.0330
1000	2.2300	2.0630
Average	0.3857	0.3111
Average speed (K bytes per second)	387.9774	481.0122

From table 1 it is seen that the presented BSS method provided good speed parameters, the average encryption time was equal 0.3857 seconds and the average decryption time was equal 0.3111 seconds, the method provided a good speed of DSF cryptography with average encryption speed equal 387.9774 K bytes per second and average decryption speed equal 481.0122 K bytes per second. It is also seen that when increasing the DSF size the ET and DT slowly grow up and the relationship between each time and the DSF size is linear as shown in figure 12.

The presented BSS method is a variable number of rounds, increasing the number of rounds increases the length of the PK and thus the security level will be increased. Increasing the number of rounds will require extra time to execute the selected additional rounds, thus the speed will be decreased, but it will be acceptable. The same selected DSFs were executed again using three rounds and the ET and DT were calculated and table 2 shows the obtained results.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

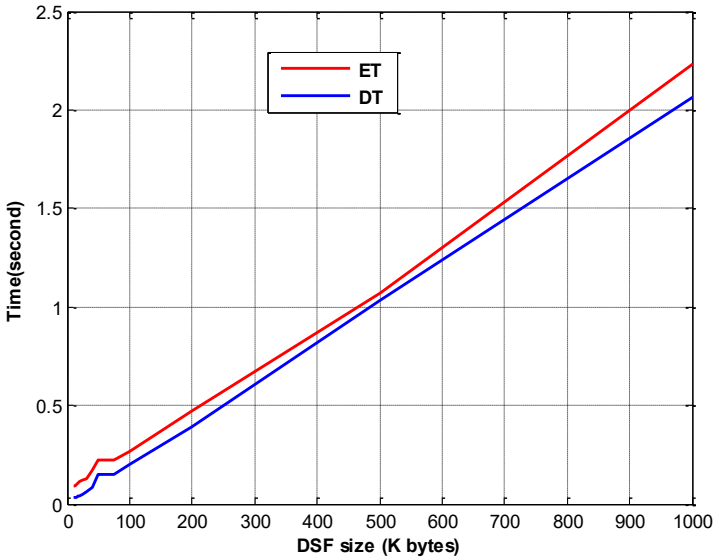

Figure 12: ET and DT vs DSF size

Table 2: BSS method speed results (3rounds)

DSF size (K bytes)	ET	DT
10	0.1280	0.0620
12	0.1450	0.0730
15	0.1590	0.0900
18	0.1760	0.1060
20	0.2130	0.1670
25	0.2110	0.1720
30	0.2420	0.1750
40	0.3050	0.2380
50	0.3650	0.3100
75	0.5050	0.4390
100	0.6610	0.5910
200	1.2370	1.1750
500	3.0990	3.0810
1000	6.3250	6.1370
Average	0.9836	0.9154
Average speed (K bytes per second)	152.1380	163.4727

From table 2 it is seen that increasing the number of rounds will decrease the speed of DSF cryptography, but the speed remains acceptable, using three rounds of DSF cryptography provided an encrypting speed of average equal 152.1380 K bytes per second and a decrypting speed of average equal 163.4727 K bytes per second.
The presented BSS method uses block size as part of the private key, and it must be noted here that this size is used to determine the number of blocks in the DSF stream of bits. Increasing the number of blocks (decreasing the block size) will lead to increase the secret key length, and thus the key generation time will be increased, and here the ET and DT will be increased, so it is recommended to use a block with big size to optimize the speed of the presented method, and to show this fact a DSF with size equal 536474 samples (4291792) was selected and implemented using one round and varying the block size (BS), the ET and DT were calculated and table 3 shows the obtained speed results:

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

Table 3: Speed results when varying BS

BS(bit)	ET(second)	DT(second)	Encryption speed (ES)(K bytes per second)	Decryption speed (DS)(K bytes per second)
50	71.5270	67.9640	58.5961	61.6680
100	15.9430	16.9920	262.8867	246.6574
250	9.9860	9.6900	419.7079	432.5287
500	8.9660	8.9250	467.4552	469.6026
750	8.8790	8.7130	472.0355	481.0287
1000	**8.7920**	**8.6620**	**476.7065**	**483.8609**
2000	8.7850	8.7380	477.0863	479.6525
5000	8.5560	8.6870	489.8554	482.4684
7500	8.5760	8.4870	488.7131	493.8380
10000	8.7320	8.4400	479.9820	496.5880

From table 3 it is seen that the optimal speed can be reached when the BS value was equal 1000 bits, decreasing this value will increase both the ET and DT, thus the speed will be decreased, so the value 1000 can be considered as an optima value (see figure 13), and here using BS greater than 1000 will keep the speed high.

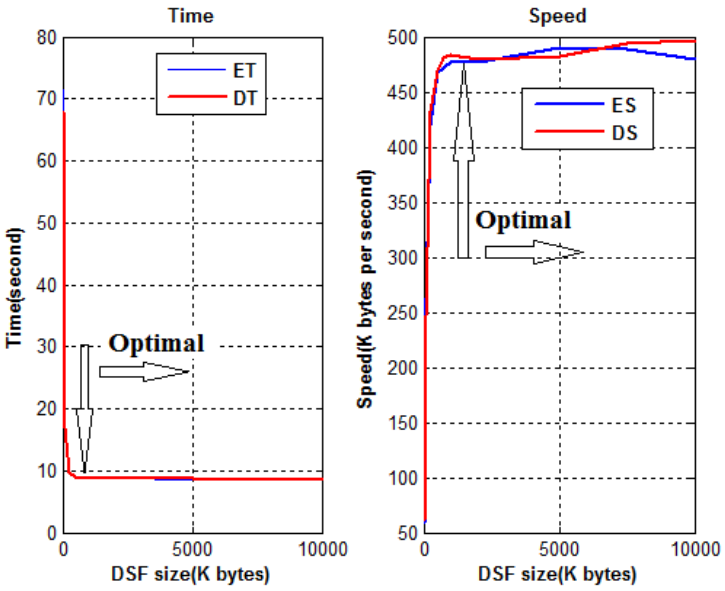

Figure 13: Crypto times and speed vs BS

The speed results of the presented BSS method were compared with other chaotic methods speed and the results of comparisons shown in table 4 show that the presented method enhanced the speed of DSF cryptography and provided a good speed up.

Table 4: Speed comparisons with chaotic methods

Method	Encryption time (second)			
	Data size: 65536 byte	Data size: 262144 byte	Average	Speed up of BSS method
Presented BSS	0.1310	0.4980	0.3145	1.0000
Ref.[1]	0.382	1.489	0.9355	2.9746
Ref.[2]	1.212	4.749	2.9805	9.4769
Ref.[4]	1.245	4.826	3.0355	9.6518
Ref.[5]	0.959	3.253	2.1060	6.6963

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

Also the speed results of the presented method were compared with the results of some standard method speed, and as shown in tables 5 and 6 the presented method enhanced the performance of standard method by decreasing the encryption time and the decryption time (see figures 14 and 15).

Table 5: ET comparisons with standard method

Method	Encryption time(second)				
	Data size(K bytes)				
	32	126	200	246	280
BSS	0.1320	0.3570	0.4690	0.5470	0.6590
DES	0.27	0.83	1.19	1.44	1.67
AES	0.15	0.46	0.72	0.95	1.12
RSA	0.13	0.52	0.74	1.11	1.39
ElGamal[7]	0.45	1.03	1.41	1.75	1.83

Table 6: DT comparisons with standard method

Method	*Decryption time(second)*				
	Data size(K bytes)				
	32	*126*	*200*	*246*	*280*
BSS	*0.0660*	*0.2490*	*0.4010*	*0.4820*	*0.5580*
DES	*0.44*	*0.65*	*0.85*	*1.23*	*1.45*
AES	*0.15*	*0.44*	*0.63*	*0.83*	*1.10*
RSA	*0.15*	*0.43*	*0.66*	*0.93*	*1.23*
ElGamal[7]	*0.43*	*0.85*	*1.13*	*1.30*	*1.64*

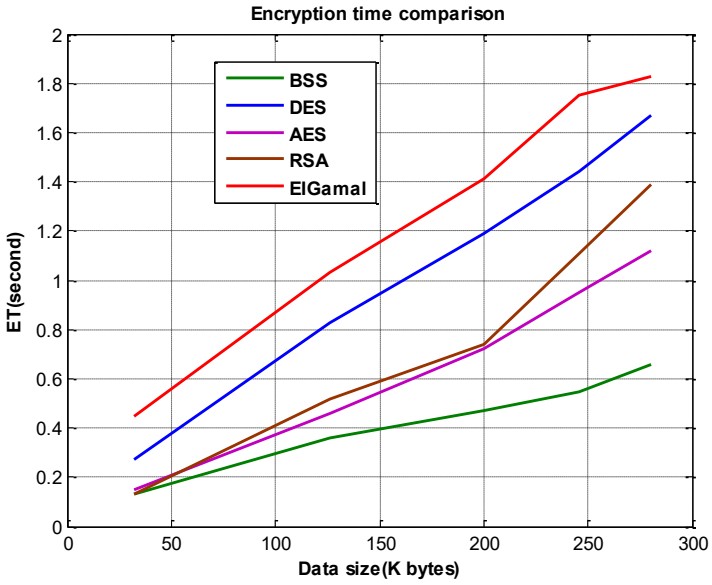

Figure 14: Various methods ET

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

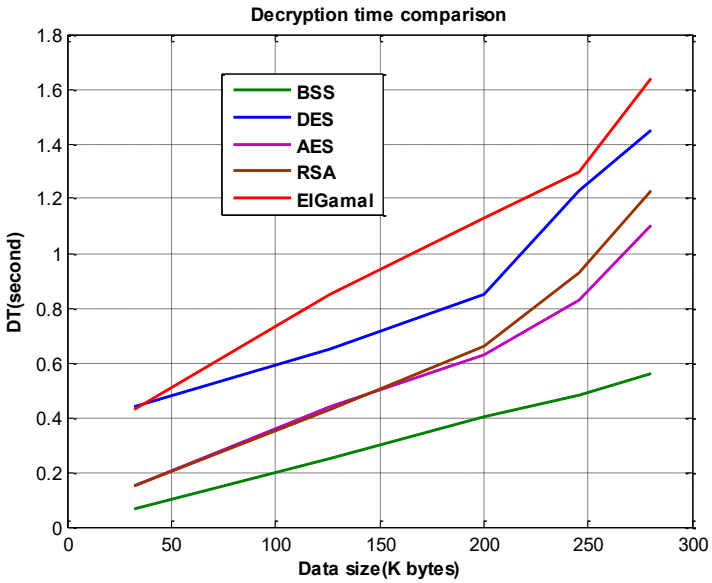

Figure 15: Various methods DT

Analysis of the data presented in Tables 4, 5 and 6 reveals the superior efficiency of the proposed method compared to conventional data cryptography techniques. The tables showcase a significant reduction in encryption time across various message lengths when employing the proposed method compared to standard methods, such as DES, AES, and RSA. This efficiency gain is particularly pronounced for long messages, underscoring the method's effectiveness in processing large volumes of data swiftly and securely. Furthermore, Figures 3 and 4 visually reinforce these findings, illustrating the disparity in encryption times between the presented BSS method and standard methods, thereby highlighting the method's efficiency in real-world cryptographic applications. The experimental validation confirmed that the pro-posed cryptography method not only meets but in many cases exceeds the performance standards of traditional algorithms. It offers a robust solution for securing data with the added benefits of high throughput and reduced processing times, making it an excellent candidate for secure communication applications that require efficient and reliable encryption.

The quality features of the presented BSS method was tested, several DSFs were selected and executed; the encrypted DSFs were always damaged, while the decrypted DSF was always the same as the associated DSF, and figure 16 shows the outputs obtained by executing one of the selected DSFs. From figure 4 the following can be seen:

- The encrypted DSF is damaged, and it was unlistenable.
- The decrypted DSF is identical to the source DSF.
- The histogram of the encrypted DSF does not match the histogram of the source DSF.
- The histogram of the decrypted DSF is the same as the histogram of the source DSF.

To insure that the presented method will satisfy the quality requirements, the quality parameters MSE, PSNR and CC where calculated. The MSE calculated between each source DSF and the associated decrypted DSF was always zero, the PSNR was always infinite while the CC was always equal 1, and this proves the decryption quality requirements of the presented method.

The encryption quality parameters were calculated and table 7 shows the obtained results (one round was used and the PK shown in figure 17 was used).

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

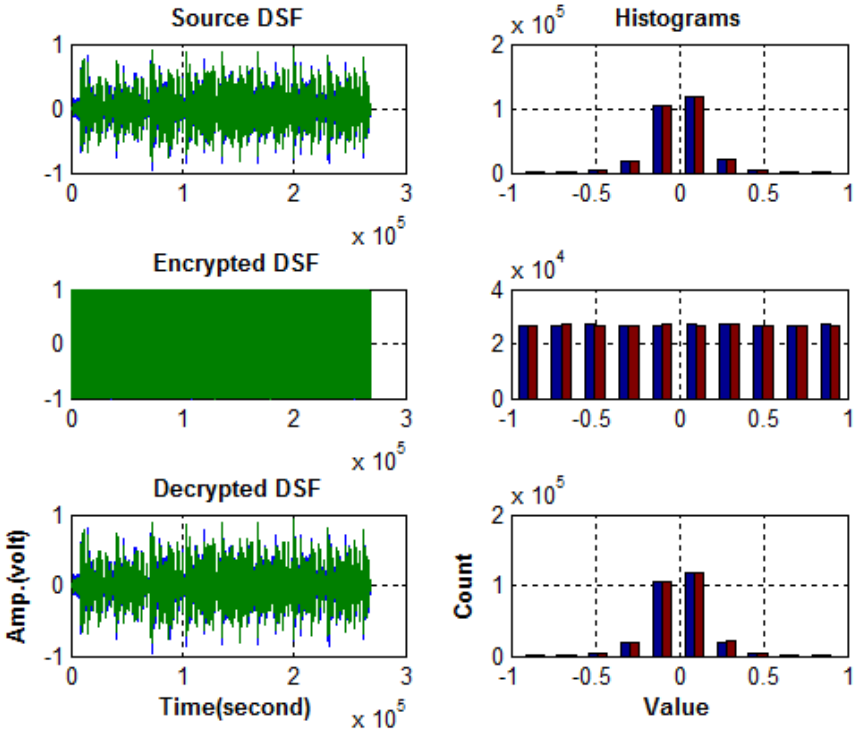

Figure 16: Sample outputs

```
%Selected PK:
BS1=1000;r1=3.77;x1=0.11;
BS2=1100;r2=3.81;x2=0.15;
BS3=1200;r3=3.67;x3=0.18;
```

Figure 17 Used PK

Table 7: Obtained encryption quality parameters

DSF size (samples)	MSE	PSNR	CC
321536	0.3339	10.9674	-0.0041
200704	0.3282	11.1350	-0.0137
227328	0.3327	11.0031	0.000437
430080	0.3322	11.0186	0.0070
536474	0.3560	10.3273	-0.0027

Upon scrutinizing Table 7, it becomes evident that the presented BSS method yields commendable results for the quality parameters (MSE, PSNR, and CC), underscoring its efficacy in preserving data integrity and fidelity throughout the encryption and decryption processes.

Increasing the number of rounds will not much affect the quality of the encrypted DSF, it will remain damaged.

The presented BSS method is very sensitive to the selected PK, the decryption part must use the same PK used in the encryption part, any changes in the PK in the decryption part will produce a damaged decrypted DSF and will be classified as a hacking attempt, and to show this fact a selected DSF was encrypted using PK1 shown in figure 18, the encrypted DSF was decrypted using each of the PKs shown in figure 7, the damaged decrypted DSFs shown in figure 19 proves that the method is very sensitive to the selected PK.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

```
%PK1:
BS1=1000;r1=3.77;x1=0.11;
%PK2:
BS1=1010;r1=3.77;x1=0.11;
%PK3:
BS1=1000;r1=3.78;x1=0.11;
%PK4:
BS1=1000;r1=3.77;x1=0.12;
```

Figure 18: Used PKs

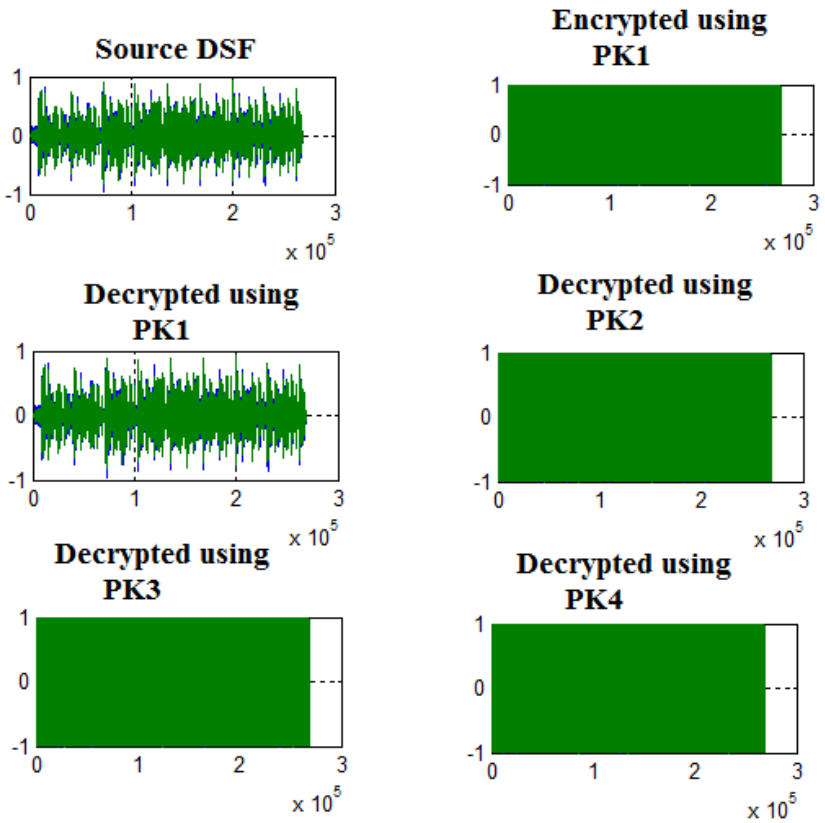

Figure 19: Obtained DSFs

CONCLUSION

A straightforward yet robust method for DSF cryptography was presented and implemented. The presented method was simple and easy to implement, it used a simple chaotic logistic map model to generate the required secret indices keys and it used a simple scattering operation to apply DSF encryption-decryption. The presented method leverages various factors, including a DSF transformation, chaotic logistic private key, a generated secret key, a sequence of operations, and the DSF blocks of bits scattering utilized for DSF encryption-decryption, to ensure robust DSF protection. Through extensive experimentation, the presented method demonstrated its ability to meet the stringent requirements of effective DSF cryptography, as evidenced by its exceptional performance in key quality parameters, such as mean square error (MSE), peak signal-to-noise ratio (PSNR), and correlation coefficient (CC). The experimental findings underscored the superiority of the presented BSS method over conventional standard DSF cryptography methods. Specifically, the presented method exhibited greater efficiency by significantly reducing encryption and decryption times, thereby

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

maximizing the speed of message cryptography. Additionally, we showcased the method's versatility by demonstrating its capability to utilize any DSF, irrespective of size. This adaptability allows for seamless integration into various applications and facilitates easy key rotation without necessitating method modifications, thus ensuring sustained security and efficiency in the message cryptography process.

REFERENCES

[1] D. Q. Lu, C. Zhu and X. Deng, "An Efficient Image Encryption Scheme Based on the LSS Chaotic Map and Single S-Box," in *IEEE Access*, vol. 8, pp. 25664-25678, 2020, doi: 10.1109/ACCESS.2020.2970806.
[2] X.-P. Zhang, R. Guo, H.-W. Chen, Z.-M. Zhao, and J.-Y. Wang, "Efficient image encryption scheme with synchronous substitution and diffusion based on double S-boxes," *Chin. Phys. B*, vol. 27, no. 8, Aug. 2018, Art. no. 080701. CrossRef Google Scholar
[3] S. Zhu, G. Wang, and C. Zhu, "A secure and fast image encryption scheme based on double chaotic S-boxes," *Entropy*, vol. 21, no. 8, p. 790, Aug. 2019.CrossRef Google Scholar
[4] X. Wang, Ü. Çavuşoğlu, S. Kacar, A. Akgul, V.-T. Pham, S. Jafari, F. Alsaadi, and X. Nguyen, "S-box based image encryption application using a chaotic system without equilibrium," *Appl. Sci.*, vol. 9, no. 4, p. 781, Feb. 2019.CrossRef Google Scholar
[5] Ü. Çavuşoğlu, S. Kaçar, I. Pehlivan, and A. Zengin, "Secure image encryption algorithm design using a novel chaos based S-Box," *Chaos, Solitons Fractals*, vol. 95, pp. 92–101, Feb. 2017. CrossRef Google Scholar
[6] Sameth, Mark (2020). *The Name : a history of the dual-gendered Hebrew name for God*. Eugene, Oregon: Wipf & Stock. pp. 5–6. ISBN 9781532693830.
[7] Faiqa Maqsood, Muhammad Mumtaz Ali, Muhammad Ahmed, Munam Ali Shah, Cryptography: A Comparative Analysis for Modern Techniques, (IJACSA) International Journal of Advanced Computer Science and Applications,vol. 8, No. 6, 2017.
[8] Majed Omar Dwairi, Amjad Hindi, Ziad A.A Al Qadi, An Efficient and Highly Secure Technique to encrypt and decrypt color images, June 2019, Engineering, Technology and Applied Science Research, 9(3):4165-4168, DOI: 10.48084/etasr.2525
[9] Motameni, M.Norouzi, M.Jahandar, & A. Hatami,"Labeling method in Steganography", Proceedings of world academy of science, engineering and technology, 24, pp.349-354, 2007. ISSN 1307-6884. http://www.waset.org/journals/waset/v30/v30-66.pdf
[10] Mohammed A.F Al Husainy, "Message Segmentation to Enhance the Security of LSB Image Steganography", International Journal of Advanced Computer Science and Applications, 3(3): 57-62, 2012.http://www.ijacsa.thesai.org
[11] Mohammed A.F Al Husainy, "Developed Segmented LSB Image Steganography", International Science and Technology Conference (ISTEC 2012), Dubai, December 13-15, 2012. http://www.iste-c.net
[12] Afjal H. Sarower; Rashed Karim; Maruf Hassan, An Image Steganography Algorithm using LSB Replacement through XOR Substitution, Computer Science:2019 International Conference on Information and Communications Technology (ICOIACT), DOI:10.1109/icoiact46704.2019.8938486.
[13] Rashad J. Rasras1, Mutaz Rasmi Abu Sara2, Ziad A. AlQadi3, Rushdi Abu zneit, Comparative Analysis of LSB, LSB2, PVD Methods of Data Steganography, International Journal of Advanced Trends in Computer Science and Engineering, vol. 8, issue 3 ,2019, https://doi.org/10.30534/ijatcse/2019/64832019
[14] Ziad A. Alqadi, Majed O. Al-Dwairi, Amjad A. Abu Jazar and Rushdi Abu Zneit, 2010, Optimized True-RGB color Image Processing, World Applied Sciences Journal8 (10): 1175-1182, ISSN 1818-4952.
[15] Waheeb, A. and Ziad AlQadi, 2009. Gray image reconstruction, Eur. J. Sci. Res., 27: 167-173.
[16] Akram A. Moustafa and Ziad A. Alqadi, Color Image Reconstruction Using A New R'G'I Model, Journal of Computer Science 5 (4): 250-254, 2009 ISSN 1549-3636.https://doi.org/10.3844/jcs.2009.250.254
[17] Musbah J. Aqel, Ziad ALQadi, Ammar Ahmed Abdullah, RGB Color Image Encryption-Decryption Using Image Segmentation and Matrix Multiplication, International Journal of Engineering & Technology, 7(3.13) (2018) 104-107.https://doi.org/10.14419/ijet.v7i3.13.16334
[18] Bilal Zahran, Ziad Alqadi, Jihad Nader, Ashraf Abu Ein,A COMPARISON BETWEEN PARALLEL ANDSEGMENTATIONMETHODS USED FOR IMAGE ENCRYPTION-DECRYPTION International Journal of Computer Science & Information Technology (IJCSIT) Vol 8, No 5,October 2016.
[19] Khaled Matrouk, Abdullah Al- Hasanat, HaithamAlasha'ary, Ziad Al-Qadi, Hasan Al-Shalabi, Analysis of Matrix Multiplication Computational Methods, European Journal of Scientific Research, ISSN 1450-216X / 1450-202X Vol.121 No.3, 2014, pp.258-266.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

[20] Ziad A.A. Alqadi, Musbah Aqel, and Ibrahiem M. M. ElEmary, Performance Analysis and Evaluation ofParallel Matrix Multiplication Algorithms, World Applied Sciences Journal 5 (2): 211-214, 2008.
[21] Z Alqadi, A Abu-Jazzar, Analysis of program methods used in optimizing matrix multiplication, Journal of Engineering, 2005
[22] Musbah J. Aqel , Ziad A. Alqadi, Ibraheim M. El Emary, Analysis of Stream Cipher Security Algorithm, Journal of Information and Computing Science Vol. 2,No. 4, 2007, pp. 288-298.
[23] J. Al-Azzeh, B. Zahran, Z. Alqadi, B. Ayyoub, M. Abu-Zaher, A Novel zero-error method to create a secret tag for an image, Journal of Theoretical and Applied Information Technology, Vol. 96. No. 13, pp. 4081-4091, 2018.
[24] Prof. Ziad A.A. Alqadi, Prof. Mohammed K. Abu Zalata, Ghazi M. Qaryouti, Comparative Analysis of Color Image Steganography, JCSMC, Vol.5, Issue. 11, November 2016, pg.37–43.
[25] M. Jose, "Hiding Image in Image Using LSB Insertion Method with Improved Security and Quality", International Journal of Science and Research, Vol. 3, No. 9, pp. 2281-2284, 2014.
[26] Emam, M. M., Aly, A. A., & Omara, F. A. An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection. International Journal of Advanced Computer Science &Applications,1(7), pp. 361-366, (2016). https://doi.org/10.14569/IJACSA.2016.070350
[27] Mohammed Abuzalata; Ziad Alqadi; Jamil Al-Azzeh; Qazem Jaber, Modified Inverse LSB Method for Highly Secure Message Hiding, IJCSMC, Vol. 8, Issue.2, February 2019, pg.93 – 103
[28] Rashad J. Rasras, Mutaz Rasmi Abu Sara, Ziad A. AlQadi, Engineering, A Methodology Based on Steganography and Cryptography to Protect Highly Secure Messages Engineering Technology & Applied Science Research, Vol.9 Issue 1, Pages 3681-3684, 2019.
[29] Zhou X, Gong W, Fu W, Jin L. 2016An improved method for LSB based color image steganography combined with cryptography. In 2016 IEEE/ACIS 15thInt. Conf. on Computer and Information Science (ICIS), Okayama, Japan, pp. 1–4 .https://doi.org/10.1109/ICIS.2016.7550955
[30] Wu D-C, Tsai W-H. A stenographic method for images by pixel value differencing. Pattern Recognition. Lett. 24, 1613–1626. 2003https://doi.org/10.1016/S0167-8655(02)00402-6
[31] Das R, Das I. Secure data transfer in IoT environment: adopting both cryptography and steganography techniques. In Proc. 2nd Int. Conf. on Research in Computational Intelligence and Communication Networks, Kolkata, India, pp. 296–301, 2016.https://doi.org/10.1109/ICRCICN.2016.7813674
[32] M. Abu-Faraj, and Z. Alqadi, "Image Encryption using Variable Length Blocks and Variable Length Private Key," International Journal of Computer Science and Mobile Computing (IJCSMC), vol. 11, Iss. 3, pp. 138-151, 2022.
[33] M. Abu-Faraj, A. Al-Hyari, and Z. Alqadi, "A Dual Approach for Audio Cryptography," Journal of Southwest Jiaotong University, vol. 57, no. 1, pp. 24-33, 2022.
[34] M. Abu-Faraj, A. Al-Hyari, and Z. Alqadi, "Complex Matrix Private Key to Enhance the Security Level of Image Cryptography," Symmetry, vol. 14, Iss. 4, pp. 664-678, 2022.
[35] M. Abu-Faraj, K. Aldebei, and Z. Alqadi, "Simple, Efficient, Highly Secure, and Multiple Pur- posed Method on Data Cryptography," Traitement du Signal, vol. 39, no. 1, pp. 173-178, 2022.
[36] M. Abu-Faraj, Khaled Aldebe, and Z. Alqadi, "Deep Machine Learning to Enhance ANN Performance: Fingerprint Classifier Case Study," Journal of Southwest Jiaotong University, vol. 56, no. 6 , pp. 685-694, 2021.
[37] M. Abu-Faraj, Z. Alqadi, and K. Aldebei, "Comparative Analysis of Fingerprint Features Ex- Traction Methods," Journal of Hunan University Natural Sciences, vol. 48, iss. 12, pp. 177-182, 2021.
[38] M. Abu-Faraj, and Z. Alqadi, "Improving the Efficiency and Scalability of Standard Meth- ods for Data Cryptography," International Journal of Computer Science and Network Security (IJCSNS), vol. 21, no.12 , pp. 451-458, 2021.
[39] Abdullah N. Olimat, Ali F. Al-Shawabkeh, Ziad A. Al-Qadi, Nijad A. Al-Najdawi, Forecasting the influence of the guided flame on the combustibility of timber species using artificial intelligence, Case Studies in Thermal Engineering, Volume 38, 2022, 102379, ISSN 2214-157X, https://doi.org/10.1016/j.csite.2022.102379.
[40] M. Abu-Faraj, and Z. Alqadi, "Image Encryption using Variable Length Blocks and Variable Length Private Key," International Journal of Computer Science and Mobile Computing (IJCSMC), vol. 11, Iss. 3, pp. 138-151, 2022.
[41] M. Abu-Faraj, A. Al-Hyari, and Z. Alqadi, "A Dual Approach for Audio Cryptography," Journal of Southwest Jiaotong University, vol. 57, no. 1, pp. 24-33, 2022.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

[42] M. Abu-Faraj, A. Al-Hyari, and Z. Alqadi, "Complex Matrix Private Key to Enhance the Security Level of Image Cryptography," Symmetry, vol. 14, Iss. 4, pp. 664-678, 2022.
[43] M. Abu-Faraj, K. Aldebei, and Z. Alqadi, "Simple, Efficient, Highly Secure, and Multiple Purr- posed Method on Data Cryptography," Traitement du Signal, vol. 39, no. 1, pp. 173-178, 2022.
[44] M. Abu-Faraj, Khaled Aldebe, and Z. Alqadi, "Deep Machine Learning to Enhance ANN Performance: Fingerprint Classifier Case Study," Journal of Southwest Jiaotong University, vol. 56, no. 6 , pp. 685-694, 2021.
[45] M. Abu-Faraj, and Z. Alqadi, "Improving the Efficiency and Scalability of Standard Meth- odds for Data Cryptography," International Journal of Computer Science and Network Security (IJCSNS), vol. 21, no.12 , pp. 451-458, 2021.
[46] J. Vilkamo and T. Bäckström, "Time-Frequency Processing: Methods and Tools," in Parametric Time-Frequency Domain Spatial Audio, V. Pulkki, S. Delikaris-Manias, and A. Politis, Eds. Wiley, 2017, pp. 3–24.
[47]. K Matrouk, A Al-Hasanat, H Alasha'ary, Ziad Al-Qadi, H Al-Shalabi, Speech fingerprint to identify isolated word person, World Applied Sciences Journal, 31 (10), 1767-1771, 2014.
[48]. Ziad alqadi, Analysis of stream cipher security algorithm, Journal of Information and Computing Science, vol. 2, issue 4, pp. 288-298, 2007.
[49]. Jamil Al-Azzeh, Bilal Zahran, Ziad Alqadi, Belal Ayyoub, Muhammed Mesleh, A Novel Based On Image Blocking Method to Encrypt-Decrypt Color, International Journal on Informatics Visualization, vol. 3, issue 1, pp. 86-93, 2019.
[50]. Musbah J Aqel, Ziad ALQadi, Ammar Ahmed Abdullah, RGB Color Image Encryption-Decryption Using Image Segmentation and Matrix Multiplication, International Journal of Engineering and Technology, vol. 7. Issue 3.13, pp. 104-107. 2018.
[51]. Jihad Nadir, Ashraf Abu Ein, Ziad Alqadi, A Technique to Encrypt-decrypt Stereo Wave File, International Journal of Computer and Information Technology, vol. 5, issue 5, pp. 465-470, 2016.
[52]. Saleh Khawatreh, Belal Ayyoub, Ashraf Abu-Ein, Ziad Alqadi, A Novel Methodology to Extract Voice Signal Features, International Journal of Computer Applications, vol. 975, pp. 8887, 2018.
[53]. Majed O. Al-Dwairi, Amjad Y. Hendi, Mohamed S. Soliman, Ziad A.A. Alqadi, A new method for voice signal features creation, International Journal of Electrical and Computer Engineering (IJECE), vol. 9. Issue 9, pp. 4092-4098, 2019.
[54]. Aws Al-Qaisi, Saleh A Khawatreh, Ahmad A Sharadqah, Ziad A Alqadi, Wave File Features Extraction Using Reduced LBP, International Journal of Electrical and Computer Engineering, vol. 8. Issue 5, pp. 2780-2787, 2018.
[55] Ayman Al-Rawashdeh, Ziad Al-Qadi, using wave equation to extract digital signal features, Engineering, Technology & Applied Science Research, vol. 8, issue 4, pp. 1356-1359, 2018.
[56]. Ashraf Abu-Ein, Ziad AA Alqadi, Jihad Nader, A TECHNIQUE OF HIDING SECRETE TEXT IN WAVE FILE, International Journal of Computer Applications, 2016
[57]. Ismail Shayeb, Ziad Alqadi, Jihad Nader, Analysis of digital voice features extraction methods, International Journal of Educational Research and Development, vol. 1, issue 4, pp. 49-55, 2019.
[58]. Jihad Nader Ahmad Sharadqh, Ziad Al-Qadi, Bilal Zahran, Experimental Investigation of Wave File Compression-Decompression, International Journal of Computer Science and Information Security, vol. 14m issue 10, pp. 774-780, 2016.
[59]. Ziad A AlQadi Amjad Y Hindi, O Dwairi Majed, PROCEDURES FOR SPEECH RECOGNITION USING LPC AND ANN, International Journal of Engineering Technology Research & Management, vol. 4, issue 2, pp. 48-55, 2020.
[60]. Majed O Al-Dwairi, A Hendi, Z AlQadi, an efficient and highly secure technique to encrypt-decrypt color images, Engineering, Technology &Applied Science Research, vol. 9, issue 3, pp. 4165-4168, 2019.
[61]. Amjad Y Hendi, Majed O Dwairi, Ziad A Al-Qadi, Mohamed S Soliman, a novel simple and highly secure method for data encryption-decryption, International Journal of Communication Networks and Information Security, vol. 11, issue 1, pp, 232-238, 2019
.[62]. Prof. Ziad Alqadi, Dr. Mohammad S. Khrisat, Dr. Amjad Hindi, Dr. Majed Omar Dwairi, USING SPEECH SIGNAL HISTOGRAM TOCREATE SIGNAL FEATURES, International Journal of Engineering Technology Research & Management, vol. 4, issue 3, pp. 144-153, 2020.
[63] M. Abu-Faraj, Z. Alqadi, and K. Aldebei, "Comparative Analysis of Fingerprint Features Ex- Traction Methods," Journal of Hunan University Natural Sciences, vol. 48, iss. 12, pp. 177-182, 2021.
[64] Alqadi, Z. (2019). A new method for voice signal features creation. International Journal of Electrical and Computer Engineering (IJECE), 9(5): 4092-4098.https://doi.org/10.11591/ijece.v9i5.pp4092-4098.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

[65] Alqadi, Z. (2009). A practical approach of selecting the edge detector parameters to achieve a good edge map of the gray image. Journal of Computer Science, 5(5): 355-362.
[66] Zaini, H., Alqadi, Z.A. (2021). Efficient WPT based speech signal protection. IJCSMC, 10(9): 53-65.https://doi.org/10.47760/ijcsmc.2021.v10i09.006.
[67] Zneit, R.A., Khrisat, M.S., Khawatreh, S.A., Alqadi, Z.(2020). Two ways to improve WPT decomposition used for image features extraction. European Journal of Scientific Research, 157(2): 195-205.
[68] Hindi, A., Qaryouti, G.M., Eltous, Y., Abuzalata, M.,Alqadi, Z. (2020). Color image compression using linear prediction coding. International Journal of Computer Science and Mobile Computing, 9(2): 13-20.
[69] Zaidan, A.A., Majeed, A., Zaidan, B.B. (2009). High securing cover-file of hidden data using statistical technique and AES encryption algorithm. World Academy of Science Engineering and Technology(WASET), 54: 468-479.
[70] Zaidan, A.A., Zaidan, B.B. (2009). Novel approach for high secure data hidden in MPEG video using public key infrastructure. International Journal of Computer and Network Security, 1(1): 1985-1553.
[71] Khalifa, O.O., Naji, A.W., Zaidan, A.A., Zaidan, B.B.,Hameed, S.A. (2010). Novel approach of hidden data inthe (unused area 2 within EXE file) using computation between cryptography and steganography. Int. J. Comput.Sci. Netw. Secur, 9(5): 294-300.
[72] Majeed, A., Mat Kiah, M.L., Madhloom, H.T., Zaidan,B.B., Zaidan, A.A. (2009). Novel approach for high secure and high rate data hidden in the image using image texture analysis. International Journal of Engineering and technology, 1(2): 63-69.http://eprints.um.edu.my/id/eprint/4951.
[73] Zaidan, A.A., Othman, F., Zaidan, B.B., Raji, R.Z.,Hasan, A.K., Naji, A.W. (2009). Securing cover-file without limitation of hidden data size using computation between cryptography and steganography. In Proceedings of the World Congress on Engineering, 1: 1-7.
[74] Aos, A.Z., Naji, A.W., Hameed, S.A., Othman, F.,Zaidan, B.B. (2009). Approved undetectable-antivirussteganography for multimedia information in PE-file. In 2009 International Association of Computer Science and Information Technology-Spring Conference, pp. 437-444. https://doi.org/10.1109/IACSIT-SC.2009.103.
[75] Zaidan, A.A., Zaidan, B.B., Abdulrazzaq, M.M., Raji,R.Z., Mohammed, S.M. (2009). Implementation stage for high securing cover-file of hidden data using computation between cryptography and steganography. International Association of Computer Science and Information Technology (IACSIT), indexing by Nielsen,Thomson ISI (ISTP), IACSIT Database, British Library and EI Compendex, 19: 482-489.
[76] Naji, A.W., Zaidan, A.A., Zaidan, B.B., Muhamadi, I.A.(2010). Novel approach for cover file of hidden data in the unused area two within EXE file using distortion techniques and advance encryption standard. Proceeding of World Academy of Science Engineering and Technology (WASET), 56(5): 498-502.
[77]. M. Bala Kumara, P. Karthikkab , N. Dhivyac , T. Gopalakrishnan, A Performance Comparison of Encryption Algorithms for Digital Images, International Journal of Engineering Research & Technology (IJERT), Vol. 3 Issue 2, February – 2014.
[78]. Lee Mariel Heucheun Yepdia, Alain Tiedeu, and Guillaume Kom, A Robust and Fast Image Encryption Scheme Based on a Mixing Technique, Security and Communication Networks, Volume 2021 |Article ID 6615708 | https://doi.org/10.1155/2021/6615708.
[79]. Z. Hua, Y. Zhou, and H. Huang, “Cosine-transform-based chaotic system for image encryption,” Information Sciences, vol. 480, pp. 403–419, 2019.
[80]. M. Asgari-chenaghlu, M.-A. Balafar, and M.-R. Feizi-Derakhshi, “A novel image encryption algorithm based on polynomial combination of chaotic maps and dynamic function generation,” Signal Processing, vol. 157, p. 1, 2019.
[81]. X. Zhang and X. Wang, Multiple-image Encryption Algorithm Based on DNA Encoding and Chaotic System, Springer, New York, NY, USA, 2019.
[82]. J. S. Zhenjun and R. Sun, “Multiple-image encryption with bit-plane decomposition and chaotic maps,” Optics and Lasers in Engineering, vol. 80, pp. 1–11, 2016.
[83] Pleacher, D. (n.d.), Calculating password entropy. Retrieved February 16, 2023, from https://www.pleacher.com/mp/mlessons/algebra/entropy.htmlPotter,
[84] Shaza D. Rihan, Ahmed Khalid Saife, Eldin F. Osman, A Performance Comparison of Encryption Algorithms AES and DES, International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 IJERTV4IS120227 www.ijert.org (This work is licensed under a Creative Commons Attribution 4.0 International License.) Vol. 4, Issue 12, December-2015.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

[85] Chunyang Sun, Erfu Wang and Bing Zhao. Image encryption scheme with compressed sensing based on a new six-dimensional non-degenerate discrete hyper-chaotic system and plaintext-related scrambling [J]. Entropy 2021, 23, 291:1–25
[86]Bingxue Jin, Liuqin Fan, Bowen Zhang, Rongqing Lei, Lingfeng Liu, Image encryption hiding algorithm based on digital time-varying delay chaos model and compression sensing technique, iScience, Volume 27, Issue 9, 2024, 110717, ISSN 2589-0042,https://doi.org/10.1016/j.isci.2024.110717.
(https://www.sciencedirect.com/science/article/pii/S2589004224019424)