THE SECURITY OF TEXT DATA BASED ON CYCLIC CODES OVER ALGEBRAIC STRUCTURE

by

Adel BAHADDAD [a*], ***Muhammad ASIF*** [b], ***M. Usman ASHRAF*** [c], ***Yousef ASIRI*** [d], ***and Salem ALKHALAF*** [e]

[a] Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia
[b] Department of Mathematics, University of Management and Technology, Sialkot Campus, Pakistan
[c] Department of Computer Science, GC Women University Sialkot, Sialkot, Pakistan
[d] College of Computer Science and Information Systems, Najran University, Najran, Saudi Arabia
[e] Department of Information Technology, College of Computer, Qassim University, Buraydah, Saudi Arabia

Original scientific paper
https://doi.org/10.2298/TSCI2406205B

The demand for network security is increasing exponentially as businesses strive to protect personal data from theft or loss. Data security is a paramount concern for both individuals and organizations engaged in various forms of communication, particularly in cyberspace due to the rise of digital computing and communication. With the rapid advancement in digital data exchange, securing information during transmission and storage has become increasingly critical. Given the extensive use of text in security agencies and industries, it is crucial to protect confidential text data from unauthorized access. This paper proposes the use of Bose Chaudhary Hochquenghem (BCH) codes over the Galois field in a modified advanced encryption standard (AES) algorithm to secure text data. Secret keys are generated using the generator polynomial of BCH codes over the Galois field, which is also applied to construct maximum distance separable (MDS) matrices. The proposed scheme enhances the mixed column operation and sub-key construction steps of the AES algorithm using BCH codes over the Galois field. The secret key, based on the designed distance of BCH codes, is difficult to predict using exhaustive key search methods. The avalanche effect test, involving single-bit changes in plaintext and secret keys, along with the popular national institute of standards and technology (NIST) test, confirms that the proposed scheme improves ciphertext encryption. Security analysis results demonstrate better encryption performance for text data. In the future, this approach could be adapted for encrypting images, audio, and video.

Key words: *AES algorithm, cryptography, cipher text, cyclic codes, Galois field*

Introduction

Nowadays cryptography and coding theory have the main part in the data security and communication channel. The communication through internet and mobile phone is rapidly increasing and occupying the wide-ranging area in daily life. There are increased numbers of unauthorized users who are trying to fetch data using illegal ways which cases the issues in data protection. Diffusion and confusion are the two basic properties required for

* Corresponding author, e-mail: dbabahaddad10@kau.edu.sa

the design of block ciphers presented by Shannon [1], Communication theory of secrecy systems. Differential cryptanalysis made sense of by Heys and Tavare in [2-4]. Subsequently, MDS frameworks give dissemination in cryptographic calculations and the primary part in the design of block codes to make them safe against the straight and differential cryptanalysis. The current age figures Shark [5], AES, Daemen and Rijmen [6], and Schneier *et al*. [7, 8] have a dispersion layer that relies upon the blend segment activity step. Lightweight MDS frameworks developed by thorough hunt from the sidekick networks are given in paper [5]. El Maraghy *et al.* [9] used AES 128-bit algorithm for optimization of speed and area. They have used 128-bit cipher key and 128 data bits as well as. The implemented hardware scheme is calculated in real time. Singh *et al.* [10] research on elliptic curve cryptography (ECC) and they implement ECC on text encryption. After modification results of image encryption for security are better. Shah *et al.* [11, 12] introduced another criterion approach to analyze the dominant *S*-boxes and non-linear *S*-boxes for degree 8 then study their weaknesses and strength to define their correctness in data encryption applications. Naseer *et al.* [13] improve multimedia security using Chaotic map and non-linear S_p boxes. Electrocardiogram signal encryption and decryption which is based on a QR code is defined by Mathivanan *et al*. [14]. Kamali *et al.* [15] modify the AES algorithm in shift row transformation. Different authors utilize multiple techniques to secure image and text data [16-33].

In this paper, we utilize BCH codes to modify the AES algorithm in mixed column operation and round key addition steps. Then results of ciphertext analyze by Avalanche effect and NIST tests. These analyses are applied to cipher-text which is encrypted by the modify AES. Mixed column matrices and round keys of the algorithm are derived from the generator polynomials of the respecting BCH codes.

Basic concepts of coding theory

Definition (Bose Chaudhary Hochquenghem codes)

The BCH codes are cyclic linear codes named after Raj Bose, Chaudhary and Hochquenghem. Let c, d, q, n be positive integers such that: $2 \le d \le n$, $q = p^m$, and $(n, q) = 1$. Let m be the smallest positive integer such that: $q^m \equiv 1 (\text{mod } n)$. Thus $n | q^m - 1$.

Let ξ be a primitive n$^{\text{th}}$ root of unity in F_{q^m}. Let $m_i(y) \in F_q[y]$ denote the minimal polynomial of ξ_i. Let $g(y)$ be the product of distinct minimal polynomials among: $m_i(y)$, $i = h, h + 1, ..., h + d - 2$, that is $g(y) = l.c.m\{m_i(y) | i = h, h + 1, ..., h + d - 2\} \in F_q[y]$.

Since $m_i(y)$ divides $y^n - 1$ for each i, it follows that $g(y)$ divides $y^n - 1$. Letn C be a cyclic code with generator polynomial $g(y)$ in the ring $F_q[y]$. Then C is called BCH code of length n over F_q.

A code C having dimension $[n, k, d]$ with generator matrix $G = [I_k | A]$, where A is a matrix of order $k \times (n - k)$ is MDS *iff* all the square sub-matrices of A are non-singular.

Theorem

Let $g(x)$ be the polynomial generator of a cyclic $[n, k]$ – code C over the field F and A be a $k \times (n - k)$ matrix whose j^{th} row is $rem_{g(x)}(x^{n-k+j-1})$, $j = 1, 2, ..., k$. Then the canon-ical form of the parity-check matrices and generator matrices of C are defined:

$$H = \left[A^T \vdots I_{n-k} \right] \text{ and } G = \left[I_k \vdots -A \right]$$

Remark

All the square sub-matrices of A are non-singular if and only if the square matrix A is an MDS matrix and a MDS matrix has only the non-zero entries.

Advanced encryption standard algorithm

The AES is a symmetric block cipher system that uses exchange or replaces network [34-36]. According to the required key length and data block length of AES can be varied. For an iteration of 10, 12, and 14 rounds, three different key length schedules, 128, 192, and 256, are used, respectively. The key size determines the level of security; as the key size increases, the security level will be increased. AES uses the round function that's composed of four different byte-oriented transformations. Key expand turns, and round change are the three main aspects of the AES algorithm. The transformation of each round is the collection of three layers add-round key layer, a non-linear layer, and the linear mixture layer. Figure 1 explains the AES encryption process [37-40]. Each round of the AES algorithm consists of the following four steps that are explained below:

– Byte substitution step
– Permutation of rows by cyclic shift
– Multiply with fixed matrix
– Bit XOR with round keys

Byte substitution

To create confusion in plain text, we replace each byte with the element of the *S*-box. This operation explains how each byte of the state matrix substitutes with another byte of the Substitution box by the substitution method. *S*-box contains 256 elements. We use different techniques to construct *S*-box.

Permutation of rows by cyclic shift

In this Transformation, the bytes of the rows of the current state matrix are left and shifted cyclically. Row 0 is unchanged, and row 1 is shifted one byte to the left. In row 2, there are two bytes left shift are performed. Similarly, we apply it to the remaining rows.

Multiply with fixed matrix

The mixed column transformation operation applies on state column by column if each column is four-term polynomials over the Galois field. The bytes in each state matrix column are hybrid by multiplying the current state matrix using a fixed polynomial matrix. This operation acts as a diffusion layer and thus fully deviations the setting of the ciphertext even if all the bytes look equivalent in appearance.

Add round key transformation

In this step, the round key is bit XOR with the output after applying mixed column operation. The round key is constructed from the original key using the key schedule process. This operation proceeds column by column at a time and adds a round-key word with every column of the state matrix. The operation thus achieved in this last segment of AES is the addition of a state matrix with round-key 10. The working of AES algorithm is shown in the fig. 1.

Proposed framework

According to the proposed algorithm, key and block sizes are fixed at 128 bits. To encrypt the plain text into cipher text, m, traditional arithmetical operations, including logical XOR and shifting methods, are used by repeating four steps 10 times. However, these steps are not constant against each round because of the difficulty of making the cryptanalysis.

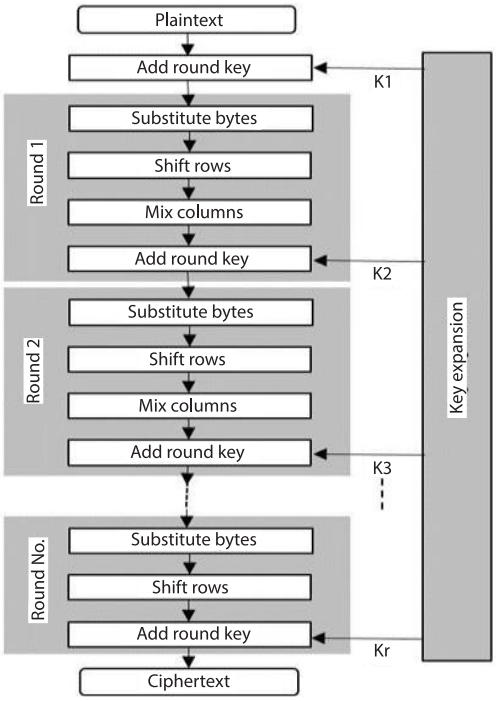

Figure 1. The fundamental AES framework

Steps for encryption text

- *Step 1*. Transform plain text data into 16 bytes and convert it into 4 × 4 matrices.
- *Step 2*. Construct subkeys from the BCH codes with 128 128 and various distances designs over the Galois field. Here, keys 0 and 1 will be used in rounds 0,1. Further, implement 10 various keys against 10 rounds.
- *Step 3*. Replace each byte of plain text data with the entries of the *S*-box.
- *Step 4*. After applying the *S*-box, shift the entries of each row to the left side. There is no change in the first row, 2nd row is shifted one place to the left, 3rd shift is two bytes on the left-hand side, and the last is shifted three
- *Step 5*. bytes to the left.
- Step 6. Construct the mixed column matrix for each round of the AES algorithm using BCH codes of length 255. Multiply the output of *Step 4* by the proposed mixed column matrix. Apply different matrices in different rounds. The simplification of this step is based on algebraic structure $GF(2^8)$.
- *Step 7*. Bit XOR the output of *Step 5* to the proposed subkeys.

Round keys structure

It has been established how to generate round keys with BCH codes over GF(27) for different predefined distances. Every generator polynomial is transformed into its 128-bit binary representation. In order to make it 128 bits long, extra bits are added or deleted from the left-hand side if it is not already. The 128-byte BCH code is then reduced to 16 bytes. As a subkey, this 16-byte string fills in. The BCH code's generator polynomial with parameters [n = 127, k = 1, d = 60] and an intended distance of 65 yields Key 1. Using the suggested approach, we obtain Key 0 as:

Key 0: = 0 171 49 22 156 132 164 219 143 65 168 203 176 235 207 191

Next, we will create the following key by utilizing a 127-length BCH code over GF(2^7) for a designed distance of 60. To accomplish this, we will convert the coefficients of the generator polynomial into a block of 8 bits each in descending order as:

00000000 10101011 00110001 00010110 10011100 10000100 10100100 11011011 10001111 01000001 10101000 11001011 10110000 11101011 11001111 10111111

Convert each byte into decimal form for round key addition, so hence key 2 is:

Key 1: 0 1 101 123 192 163 7 249 56 40 16 229 154 109 22 187

Similarly, we construct all keys with the help of BCH codes over the Galois field for different designed distances. All Keys are shown:

Key 2: 0 0 3 146 27 208 157 120 3 122 83 250 137 174 174 43

Key 3: 0 0 0 5 16 109 174 23 166 30 82 12 96 106 78 41

Key 4: 0 0 0 0 13 83 6 214 191 219 200 87 71 25 231 13
Key 5: 0 0 0 0 0 25 161 99 10 46 46 13 22 111 12 93
Key 6: 0 0 0 0 0 0 41 19 31 9 172 122 28 6 238 111
Key 7: 0 0 0 0 0 0 0 65 218 145 157 158 251 54 166 153
Key 8: 0 0 0 0 0 0 0 0 244 132 85 24 185 88 42 31
Key 9: 0 0 0 0 0 0 0 0 1 43 127 137 19 147 44 17
Key 10:0 0 0 0 0 0 0 0 0 2 146 195 22 238 162 115

Construction of mixed column matrix

Constructing the mixed column matrix is crucial in AES as it contributes to confusion and diffusion.

Step 1. Find generator polynomial of n BCH code for designed distance, δ, where $n = 2^m - 1$ and m are the highest power of primitive polynomials.

Step 2. Choose a value δ satisfying: $l + 1 \leq \delta \leq 2^m - l$.

Step 3. Calculate the dimension of the code $k = n - r$, where r is the highest power in the polynomial generator of BCH code.

Step 4. Divide the $x^{n-k+i-}1$ where $i = 1, 2, ..., k$ by generator polynomial and get remainder polynomial.

Step 5. Each remainder polynomial is converted into binary form and divided into blocks of 8 bits, then converted into decimal form and written into a matrix.

Step 6. The coefficients of the remainder polynomial in decimal form are written into an $l \times l$ matrix, ensuring that the resulting matrix is non-singular.

Example

Assume that we must develop a blended segment framework with the assistance of BCH code of length 255 with planned distance $\delta = 119$. Here we take $l = 4$ so that δ fulfilling the disparity $5 \leq \delta \leq 252$. Generator polynomial for BCH code with boundaries [$n = 255$, $k = 13$, $\delta = 119$], The coefficients of generator polynomial is as:

1011010100110011100000101000101111111110010101110111111001011001100001001111110110111000000111011010111111010001101110001000010111010000101100111001000011000010000010010000100100101111001100001110100001100010001000100101001001111101010100001001010111

From section *Theorem*, we calculate: $g_{BCH}(x)(x^{n-k+i-1})$, where $i = 1, ..., 13$, that is, $remg_{(BCH)}(x)(x^{i+241})$.

Coefficients of polynomial $remg_{(BCH)}(x)(x^{i+241})$ into a block of 8 bits:

11101001 00010101 11110100 10100100 01000100 01100001 01110000 11001111 01001001 00001001 00000100 00110001 00111001 10100001 01110100 00100011 10110001 01111110 10110111 00000011 10110111 11100100 00110011 01001111 11011101 01001111 11111010 00101000 00111001 10010101 110100100

$$\boldsymbol{A} = \begin{bmatrix} 11101001 & 01000100 & 01001001 & 00111001 \\ 00010101 & 01100001 & 00001001 & 10100001 \\ 11110100 & 01110000 & 00000100 & 01110100 \\ 10100100 & 11001111 & 00110001 & 00100011 \end{bmatrix}$$

Now, we covert each block into decimal form:

$$A = \begin{bmatrix} 233 & 68 & 73 & 57 \\ 21 & 97 & 9 & 161 \\ 244 & 112 & 4 & 116 \\ 164 & 207 & 49 & 35 \end{bmatrix}$$

This is the required column matrix that is used in AES for the security of data.

Similarly, we construct all nine mixed column matrices for each round except the 10th round by BCH codes for distinctly designed distances to use in the AES algorithm for text encryption.

$$A_1 = \begin{bmatrix} 221 & 104 & 182 & 89 \\ 110 & 180 & 91 & 44 \\ 234 & 50 & 155 & 207 \\ 168 & 113 & 251 & 190 \end{bmatrix}, A_2 = \begin{bmatrix} 212 & 117 & 117 & 145 \\ 190 & 79 & 207 & 89 \\ 95 & 39 & 231 & 172 \\ 251 & 230 & 134 & 71 \end{bmatrix}, A_3 = \begin{bmatrix} 148 & 114 & 86 & 6 \\ 74 & 57 & 43 & 3 \\ 177 & 110 & 195 & 135 \\ 88 & 183 & 87 & 195 \end{bmatrix}$$

$$A_4 = \begin{bmatrix} 176 & 231 & 152 & 226 \\ 232 & 148 & 84 & 147 \\ 196 & 173 & 178 & 171 \\ 98 & 86 & 217 & 85 \end{bmatrix}, A_5 = \begin{bmatrix} 186 & 48 & 246 & 104 \\ 231 & 40 & 141 & 92 \\ 201 & 164 & 11 & 198 \\ 222 & 226 & 174 & 11 \end{bmatrix}, A_6 = \begin{bmatrix} 246 & 119 & 96 & 56 \\ 123 & 59 & 176 & 28 \\ 203 & 234 & 184 & 54 \\ 101 & 245 & 92 & 27 \end{bmatrix}$$

$$A_7 = \begin{bmatrix} 153 & 101 & 108 & 223 \\ 76 & 178 & 182 & 111 \\ 38 & 89 & 91 & 55 \\ 19 & 45 & 173 & 155 \end{bmatrix}, A_8 = \begin{bmatrix} 248 & 84 & 26 & 157 \\ 132 & 126 & 23 & 83 \\ 66 & 63 & 11 & 233 \\ 33 & 31 & 133 & 244 \end{bmatrix}, A_9 = \begin{bmatrix} 136 & 52 & 201 & 200 \\ 68 & 26 & 100 & 228 \\ 34 & 13 & 50 & 114 \\ 153 & 50 & 80 & 241 \end{bmatrix}$$

Texture encryption using modified AES algorithm

Suppose we want to send a code in plain text ONE TWO NINE ONE, but before sending, we want to secure this text data using the proposed scheme modified AES algorithm. Select 128 bits key for the plain text of 128 bits, then perform 10 rounds using a modified AES algorithm and use different mixed column matrices in each round (except the last round) for better encryption. Convert each plain text letter into hex decimals and perform the modified AES encryption scheme. The round wise results of encryption scheme are shown in tab. 1.

Text Encryption analyses

Avalanche effect

Every encryption method has its weak and strong arguments. We must identify the weaknesses and strengths to apply the appropriate-ate method in a specific application. Therefore, the analyses of these methods are critically compulsory. Every encryption technique guarantees that a small alteration the key or the plaintext should result in a significant alteration the ciphertext. A single-bit change in the key or plain text that results in multiple bits of change in the ciphertext is known as the avalanche effect. Tables 2 and 3 demonstrate how the avalanche effect, which is caused by a single-bit fluctuation in the plaintext while maintaining a fixed encryption key and a one-bit change in the key while maintaining the plain text unchanged, is used to estimate the strength of the suggested technique. An equation can be used to calculate the avalanche effect:

$$\text{Avalanche effect} = \frac{\text{Number of flipped bits in the ciphertext}}{\text{Number of total bits in the ciphertext}} \quad (1)$$

Table 1. Round-wise text encryption

Round#1	Plain text = 4f 4e 65 20 54 77 6f 20 4e 69 6e 65 20 4f 4e 65 Cipher text: 7e 0 f4 4 7f cf 3e e8 f7 d5 fd 8a 8c c7 9d df
Round#2	Plain text = 7e 0 f4 4 7f cf 3e e8 f7 d5 fd 8a 8c c7 9d df Cipher text: 26 b5 54 c4 71 3e 5b 4b 77 d8 ee bf a8 45 1 f7
Round#3	Plain text = 26 b5 54 c4 71 3e 5b 4b 77 d8 ee bf a8 45 1 f7 Cipher text: 56 49 9d 94 e6 8e 39 fe 6d 17 f1 b5 3b 10 f2 71
Round#4	Plain text = 56 49 9d 94 e6 8e 39 fe 6d 17 f1 b5 3b 10 f2 71 Cipher text: 4 36 c3 0 3d 75 34 d0 51 f3 e2 23 cf 86 4a 62
Round#5	Plain text = 4 36 c3 0 3d 75 34 d0 51 f3 e2 23 cf 86 4a 62 Cipher text: 6d d6 19 77 23 a6 e1 d8 6a 7e 43 1 7c 30 57 11
Round#6	Plain text = 6d d6 19 77 23 a6 e1 d8 6a 7e 43 1 7c 30 57 11 Cipher text: b9 68 5 7b 52 7b 66 53 7e d5 16 36 1e 5 88 6a
Round#7	Plain text = b9 68 5 7b 52 7b 66 53 7e d5 16 36 1e 5 88 6a Cipher text: ea 9 88 ac 87 a5 42 da 43 e7 5d d9 3d 5f 90 2d
Round#8	Plain text = ea 9 88 ac 87 a5 42 da 43 e7 5d d9 3d 5f 90 2d Cipher text: e5 64 5e 14 5b 3b 55 a8 2d d3 55 20 3e 63 2d a8
Round#9	Plain text = e5 64 5e 14 5b 3b 55 a8 2d d3 55 20 3e 63 2d a8 Cipher text: 15 35 97 5c ba e2 71 5f 4 44 71 d8 80 6d 53 62
Round#10	Plain text =15 35 97 5c ba e2 71 5f 4 44 71 d8 80 6d 53 62 Cipher text: 59 98 a6 aa f4 1b ed 4a f2 3e 1a c db 78 1 12

Table 2. Avalanche effect test for change in plain text

Rounds	Plain text and cipher text	Number of bits that differ	Avalanche [%] of proposed AES
0	4f4e652054776f204e696e65204f4e65 4e4e652054776f204e696e65204f4e65	1	
1	7e00f4047fcf3ee8f7d5fd8a8cc79ddf d04a48ce87838e7f42f5669d7182c451	66	51.56
2	26b554c4713e5b4b77d8eebfa84501f7 000003921bd09d78037a53fa89aeae2b	70	54.69
3	56499d94e68e39fe6d17f1b53b10f271 793ee972c33a6d31fd5ec968d93dd705	65	50.78
4	0436c3003d7534d051f3e223cf864a62 2766ecf7edc4c712062f2ec36e939866	61	47.66
5	6dd6197723a6e1d86a7e43017c305711 f49a593125d9bbcc933be4ba7743ea82	64	50
6	b968057b527b66537ed516361e05886a 97b2baba6fc9dc8c5a34e8a3377f9536	73	57.03
7	ea0988ac87a542da43e75dd93d5f902d 4143037c607d9ed9543bab1177ecdb20	65	50.78
8	e5645e145b3b55a82dd355203e632da8 8e6513d9db4e5280bd284f010d04b64e	59	46.09
9	1535975cbae2715f044471d8806d5362 f20f0e00a89fa1150a601f13ac0f93c2	57	44.53
10	5998a6aaf41bed4af23e1a0cdb780112 89dbc025c2d0dc636774399a8798900e	57	44.53

Table 3. Avalanche effect test for change in key

Rounds	Plain text and cipher text	Number of bits that differ	Avalanche [%] of proposed AES
0	4f4e652054776f204e696e65204f4e65 4f4e652054776f204e696e65204f4e65	1	
1	7e00f4047fcf3ee8f7d5fd8a8cc79ddf 9b278f517fcf3ee8f7d5fd8a8cc79ddf	69	53.91
2	26b554c4713e5b4b77d8eebfa84501f7 a577394c900f545f80b8b044775184d9	63	49.22
3	56499d94e68e39fe6d17f1b53b10f271 0f0dbf745e5c963f9f01f692fdccbffe	61	47.66
4	0436c3003d7534d051f3e223cf864a62 2d4a37542accbeb9ce8319f81a98b314	74	57.81
5	6dd6197723a6e1d86a7e43017c305711 04a964f2e72ec03945070d00a1672544	65	50.78
6	b968057b527b66537ed516361e05886a e1f7dec77d51155de365093fce5e304e	65	50.78
7	ea0988ac87a542da43e75dd93d5f902d e1f7dec77d513c0f26fd38db296e78b8	66	51.56
8	e5645e145b3b55a82dd355203e632da8 b69ecb5a4c14e2fa18bc356fec7b1e7c	67	52.34
9	1535975cbae2715f044471d8806d5362 8533825f612b689bab1539687aeee7d5	58	45.31
10	5998a6aaf41bed4af23e1a0cdb780112 97f11203ef5994cf622a81d7cc2de736	61	47.66

In tab. 1, we apply the avalanche effect by altering a single bit in plain text, keeping it unchanged in the secret key, and then performing all the rounds of the proposed AES algorithm. In tab. 2, we flipped a single bit in the secret key and keep unchanged in plain text, then counted the number of bits that differed in each round. From tabs. 2 and 3, we can conclude that the number of bits flipped is almost an average of 50% in cipher text.

NIST statistical test

The discrete Fourier transform (spectral) test

It determines the sequence's periodic structures that would indicate a departure from the randomness assumption. The goal is to find the total number of peaks that are more than 95% brink and that deviate considerably from 5%.

The non-overlapping template matching test

It finds generators that produce further instances of the specified non-periodic form. To find an accurate m-bit form for both overlapping and non-overlapping template-matching test windows, *m*-bit is utilized. If the necessary form cannot be found, the window slips a single bit. However, if the precise form is located and the search resumes, the window will be reset to the bit.

The approximate entropy test

The approximate entropy test, on the other hand, focuses on the frequency of all overlapping (possible) *m*-bit forms across the entire sequence. This test aims to compare the fre-

quency of blocks of two consecutive overlapping lengths against the predicted outcomes for random sequences.

The Cumulative Sums Test

In the Cumulative Sums test, the cumulative sum of adjusted digits (–1,1) is used to determine the number of highest excursions of a random walk represented in a sequence. Finding out if the cumulative sum of partial sequence occurrences in the random sequence is equivalent to limited numbers is the main goal of the test. This random walk's excursion should ideally be around zero, but it will be far from zero for non-random sequences. Finding out if the sum of the partial sequences that occur in the tested sequence is too small or too large is the primary goal of the cumulative sums test.

Table 4 explains that NIST statistical tests to check the randomness in ciphered text using the proposed scheme of the AES algorithm. The results show that cipher text passes the statistical randomness tests.

Table 4. The NIST statistical tests

Statistical test	Decision
The discrete fourier transform (spectral)	Test passed
The non-overlapping template matching	Test passed
The approximate entropy	Test passed
The cumulative sums (forward)	Test passed
The cumulative sums (reverse)	Test passed

Ciphertext attack

In cases where the cryptanalyst is aware of the ciphertext and encryption techniques but does not possess the private key required for decryption, brute-force attacks are often considered. However, these attacks are typically ineffective for obtaining the plain text since decrypting the ciphered message could take many years, particularly if the key size is excessively large. In the unlikely event that the original message is eventually deciphered, its value may be insignificant by that point.

Known plaintext attack

The private key is used to design the encryption algorithm, ciphertext, and one or more ciphertext-plaintext pairs, all recognized by the cryptanalyst. The use of BCH codes results in different ciphertexts for the same message, which makes it impossible for known plaintext attacks to be successful.

Conclusion

The paper defines the text encryption scheme using a novel technique based on the AES algorithm and BCH codes over the Galois field. We have utilized the BCH codes by using Galois field to construct round keys and mixed column matrices for a modified AES algorithm, then encrypted the text using the proposed algorithm. The round keys are constructed by using generator polynomial of the BCH codes corresponding different designed distances. The avalanche effect was applied to the ciphertext in each round, resulting in a significant change in the ciphered text with even a small change in plain text. The results, tab. 2, suggest that this

approach provides a higher level of security. Table 3, specifies that a single-bit change in the secret key causes a big change in the ciphered text, and the use of the proposed scheme passed the five NIST tests, as shown in tab. 4. These findings demonstrate that the proposed method provides better text data security and prevents unauthorized access. In future, this algorithm can be used in intelligence agencies, forensics, and military communication and may be extended to video and audio encryption.

Acknowledgement

This research work was funded by Institutional Fund Projects under grant no, (IFPIP 1190-611-1443). The authors gratefully acknowledge technical and financial support provided by the Ministry of Education and King Abdulaziz University, DSR, Jeddah, Saudi Arabia.

References

[1] Shannon, C. E., Communication Theory of Secrecy Systems, *Bell System Technical Journal*, *28* (1949), 4, pp. 656-715
[2] Heys, H. M., Tavares, S. E., The Design of Substitution-Permutation Networks Resistant to Differential and Linear Cryptanalysis, *Proceedings*, 2nd ACM Conference on Computer and Communications Security, Fairfax, Va, USA, 1994, pp. 148-155
[3] Heys, H. M., Tavares, S. E., The Design of Product Ciphers Resistant to Differential and Linear Cryptanalysis, *Journal of Cryptology*, *9* (1996), 1, pp. 1-19
[4] Heys, H .M., Tavares, S. E., Avalanche Characteristics Oo Substitution-Permutation Encryption Networks, *IEEE Transactions on Computers*, *44* (1995), 9, pp. 1131-1139
[5] Rijmen, V., *et al*., The Cipher SHARK, In Fast Software Encryption: *Proceedings*, 3rd International Workshop, Cambridge, UK, 1996, pp. 99-111
[6] Daemen, J., Rijmen, V., The Rijndael Block Cipher: AES Proposal, *Proceedings*, 1st Candidate Conference (AeS1), London, UK, 1999, pp. 343-348
[7] Schneier, B., *et al*., Twofish: A 128-Bit Block Cipher, *NIST AES Proposal*, *15* (1998), 1, pp. 23-91
[8] Schneier, B., *et al*., The Twofish Team's Final Comments on AES Selection, *AES Round*, *2* (2000), 1, pp. 1-13
[9] El Maraghy, M., *et al*., Real-Time Efficient FPGA Implementation of AES Algorithm, *Proceedings*, IEEE International SOC Conference, Erlangen, Germany, 2013, pp. 203-208
[10] Singh, L. D., Singh, K. M., Implementation of Text Encryption Using Elliptic Curve Cryptography, *Procedia Computer Science*, *54* (2015), Dec., pp. 73-82
[11] Shah, T., *et al*., Statistical Analysis of S-Box in Image Encryption Applications Based on Majority Logic Criterion*, International Journal of Physical Sciences*, *6* (2011), 16, pp. 4110-4127
[12] Shah, T., Shah, D., Construction of Highly Non-Linear S-Boxes for Degree 8 Primitive Irreducible Polynomials over $\mathbb{Z}2$, *Multimedia Tools and Applications*, *78* (2019), 2, pp. 1219-1234
[13] Naseer, Y., *et al*., A Novel Algorithm of Constructing Highly Non-linear Sp-boxes, *Cryptography*, *3* (2019), 1, pp. 1-6
[14] Mathivanan, P., *et al*., The QR Code-Based ECG Signal Encryption/Decryption Algorithm, *Cryptologia*, *43* (2019), 3, pp. 233-253
[15] Kamali, S. H., *et al*., A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption, *Proceedings*, International Conference on Electronics and Information Engineering, 2010, Kyoto, Japan, Vol. 1, pp. V1-141
[16] Asif, M., Shah, T., The BCH Codes with Computational Approach and Its Applications in Image Encryption, *Journal of Intelligent and Fuzzy Systems*, *37* (2019), 4, pp. 3925-3939
[17] Gao, S., *et a*l., Asynchronous Updating Boolean Network Encryption Algorithm, *IEEE Transactions on Circuits and Systems for Video Technology*, *33* (2023), 8, pp. 4388-4400
[18] Gao., S., *et al.*, A 3-D Model Encryption Scheme Based on a Cascaded Chaotic System, *Signal Processing*, *202* (2023), 108745
[19] Gao, S., *et al*., The EFR-CSTP: Encryption for Face Recognition Based on the Chaos and Semi-Tensor Product Theory, *Information Sciences*, *621* (2023), Apr., pp. 766-781
[20] Alanazi, A. S., *et al*., Cryptanalysis of Novel Image Encryption Scheme Based on Multiple Chaotic Substitution boxes, *IEEE Access*, *9* (2021), June, pp. 93795-93802

[21] Khan, M., *et al*., An Efficient Image Encryption Scheme Based on Double Affine Substitution Box and Chaotic System, *Integration*, *81* (2021), Nov., pp. 108-122
[22] Asif, M., *et al*., A Novel Image Encryption Technique Based on Mobius Transformation, *Computational Intelligence and Neuroscience*, *2021* (2021), 1, pp. 1-14
[23] Naseer, Y., *et al*., Advance Image Encryption Technique Utilizing Compression, Dynamical System and S-Boxes, *Mathematics and Computers in Simulation*, *178* (2020), Dec., pp. 207-217
[24] Naseer, Y., *et al.*, A Novel Approach to Improve Multimedia Security Utilizing 3-D Mixed Chaotic Map, *Microprocessors and Microsystems*, *65* (2019), Mar., pp. 1-6
[25] Naseer, Y., *et al.*, A Novel Hybrid Permutation Substitution Base Colored Image Encryption Scheme for Multimedia Data, *Journal of Information Security and Applications*, *59* (2021), 102829
[26] Khan, M., *et al*., An Efficient Method for the Construction of Block Cipher with Multi-Chaotic Systems, *Non-Linear Dynamics*, *71* (2013), 3, pp. 489-492
[27] Khan, M., Masood, F., A Novel Chaotic Image Encryption Technique Based on Multiple Discrete Dynamical Maps, *Multimedia Tools and Applications*, *78* (2019), 18, pp. 26203-26222
[28] Hussain, I., *et a*l., A Novel Image Encryption Algorithm Based on Chaotic Maps and GF (28) Exponent Transformation, *Non-Linear Dynamics*, *72* (2013), 1, pp. 399-406
[29] Hussain, I., *et al*., Image Encryption Algorithm Based on PGL (2, GF (28)) S-Boxes and TD-ERCS Chaotic Sequence, *Non-linear Dynamics*, *70* (2012), 1, pp.181-198
[30] Rayarikar, R., *et al*., The SMS Encryption Using AES Algorithm on Android, *International Journal of Computer Applications*, *50* (2012), 19, pp. 12-17
[31] Padate, R., Patel, A., Encryption and Decryption of Text Using AES Algorithm, *International Journal of Emerging Technology and Advanced Engineering*, 4 (2014) 5, pp. 54-69
[32] Mahboob, A., *et al.*, A Cryptographic Scheme for Construction of Substitution Boxes Using Quantic Fractional Transformation, *IEEE Access*, *10* (2022), Dec., pp. 132908-132916
[33] Khalid, I., *et al*., An Integrated Image Encryption Scheme Based on Elliptic Curve, *IEEE Access*, *11* (2022), Dec., pp. 5483-5501
[34] Abdullah, A. M., Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data, *Cryptography and Network Security*, *16* (2017), 1, 11
[35] Alemami, Y., *et al*., Advanced Approach for Encryption Using Advanced Encryption Standard with Chaotic Map, *Int. J. Electr. Comput. Eng*, *13* (2023), 2, 1708
[36] Asif, M., *et al*., A Novel Image Encryption Technique Based on Cyclic Codes over Galois Field, in: *Computational Intelligence and Neuroscience*, Wiley, New York, USA, 2022, pp. 1-9
[37] Hussain, S., Redesigning the Serpent Algorithm by PA-Loop and its Image Encryption Application, *IEEE Access*, *11* (2023), Mar., pp. 29698-29710
[38] Abu-Faraj, M., *et al*., Increasing the Security of Transmitted Text Messages Using Chaotic Key and Image Key Cryptography, *International Journal of Data and Network Science*, *7* (2023), 2, pp. 809-820
[39] Kumar, M., *et al.*, Enhanced Digital Image and Text Data Security Using Hybrid Model of LSB Steganography and AES Cryptography Technique, *Proceedings*, 2nd International Conference on Artificial Intelligence and Smart Energy (ICAIS), Coimbatore, India, 2022, pp. 1453-1457
[40] Noor, N. S., *et al*., A Fast Text-to-Image Encryption-Decryption Algorithm for Secure Network Communication, *Computers*, *11* (2022), 3, pp. 1-16

Paper submitted: July 13, 2024
Paper revised: October 5, 2024
Paper accepted: November 2, 2024