Institute of Information and Computational Technologies

ISSN : 2788-7677 (Online)
ISSN : 2788-7987 (Print)

ADVANCED TECHNOLOGIES AND COMPUTER SCIENCE

2021
№4

www.atcs.iict.kz

Institute of Information and Computational Technologies

Advanced Technologies and computer science

№4

Almaty 2021

ISSN: 2788-7677 (Online)
ISSN : 2788-7987 (Print)

Institute of Information and Computational Technologies,

Advanced Technologies and computer science

28 Shevchenko str., Almaty,Republic of Kazakhstan
7 (727) 272-37-11
atcs@iict.kz

About the Journal

Advance technologies and computer science is a bilingual scientific peer-reviewed, interdisciplinary, electronic journal of open access, including thematic areas:

- Section **"Applied mathematics, computer science and control theory"** includes papers describing modern problems in these areas.
- Section **"Information and telecommunication technologies"** also includes the following topics:
    - Data transmission systems and networks.
    - Internet technologies.
    - Cloud technologies.
    - Parallel computing.
    - Distributed computing.
    - Supercomputer and cluster systems.
    - Big data processing (Big-data).
    - Geographic Information Systems and Technologies.
- In the section **"Artificial intelligence technologies"** in addition to technology, there are works on topics:
    - Intelligent Management Systems.
    - Speech technology and computer linguistics.
    - Pattern Recognition and Image Processing.
    - Bioinformatics and biometric systems.
    - Human-machine interaction.
    - Machine learning.
    - Intelligent Robotic Systems.
- The section **"Information Security and Data Protection"** also covers topics:
    - Software and hardware information protection.
    - Mathematical methods for ensuring information security of complex systems.
- The section **"Modeling and optimization of complex systems and business processes"** may include:
    - Computational mathematics, numerical analysis and programming, mathematical logic.
    - Theory of Statistics.
    - Statistical Methods.

Contents

UDC 004.02
IRSTI 20.53.15

ALGORITHM FOR OCR TEXT SEARCHING

Mirzakhmet Syzdykov[1], Santanu Kumar Patro[2]

[1]al-Farabi Kazakh National University, Almaty, Kazakhstan
[2]Berhampur University, Odisha, India
[1]mspmail598@gmail.com, [2]ksantanupatro@gmail.com
[1]ORCID ID: https://orcid.org/0000-0002-8086-775X
[2]ORCID ID: https://orcid.org/0000-0002-7917-4841

Abstract. The optical character recognition (OCR) is the modern global trend in the digital world. However, due to the errors in character recognition device, this could be almost impossible to obtain user friendly and readable version of the obtained data. For this reason, in this article we present the algorithm for effective text searching in extracted OCR thread. The novel technique is simply used based upon the sliding algorithm with error corrections, which could be also applied to the dictionary data: here this technique is based on the usage of window to search the matching and the Tesseract OCR is used as an OCR engine. In this article we also show that this algorithm is applicable only when the change character error is present. The overview of the past work is also given with respect to the classically known algorithms like Knuth-Morris-Pratt (KMP) or Boyer-Moore (BM). We also show that our algorithm works efficiently in linear polynomial time.

Keywords: Optical Character Recognition, Linear Algorithm, Mathematical Probability.

Introduction

The most known algorithms to the present time for pattern string matching, i.e. the problem of finding the occurrences of pattern in the matching string, like Knuth-Morriss-Pratt [1] and Boyer-Moore [2] were adapted for the digital patterns, when pattern can be taken from the scanned image [3, 4]. We present the linear error-prune algorithm for OCR text matching.

The matching cost can be computed using variety of techniques, for example, Hamming distance [5]. For experimental purpose as it was stated in the abstract Tesseract OCR [6] engine is used. However, the Hamming distance is good for low-cost computing, while the approach described in this paper can be used for large data. To handle the large data thread, we have used the windowing technique, so by this method the necessary data for the pre-defined time interval can be obtained as:

Window [1….t] = Data * Time[1..t] (1).

From the obtained data the penalty can be computed. This penalty is the measure of equivalence between searching text and scrambled data, possibly by OCR engine. So that the following holds true:

Penalty [Data [1…t]] == A ~ B (2),

where:

‘A’ is the searching text and
‘B’ is scrambled data.

Now we would like to present a short introduction to the naive approach and, in overall, saying, this paper is organized in such a way that after presenting a short introduction, we give the Java code for this method. After which we present the scalable window approach, with its codes. In the very next section, we present its application part, i.e the experimental results.

Naive Approach

The naive approach is nothing but to calculate the distance between two words. This method has a good application when number of symbols (or the weight of word) in text to be searched is

small. Obviously by this method we get the magnitude equal to the weight of text. To compute this distance the bi-linear search is executed at every position in scrambled text. The cost here is, thus, a cumulative sum of penalties at every step when symbols coincide. This can be written as:

Cost (A, B) = SUM {1.0 / Distance[X[1], X[2]]} (3),

where,

A, B are words and

X[1], X[2] are positions of two consecutive matchings.

It's to be noted that the algorithm experimentally produces good results for low-cost pattern (word A). Even the java code can be used for this purpose: so now we would like to present its coding part in Java.

The java code for naive approach:

```
public static SearchResult query_exact (String text, String query_text, String text_0, String query_text_0) {
        float max_scal_match = 0.0f;
        int best_match_start = -1;
        int best_match_end = -1;
        int best_page_line = -1;
        int best_page_offset = -1;
        int best_page = -1;
        int page_line = 0;
        int page_offset = 0;
        int page = 0;

        for (int i = 0; i < text.length(); ++i) {
                float scal_match = 0.0f;
                int last_match_pos = -1;
                for (int j = 0, k = i; j < query_text.length() && k < text.length(); ++j, ++k) {
                        if (text.charAt(k) == '\n') {
                                ++page_line;
                                page_offset = 0;
                        } else if (((int)text.charAt(k)) == 12) {
                                ++page;
                                page_line = page_offset = 0;
                        }

                        if (text.charAt(k) == query_text.charAt(j)) {
                                int gap = 1;
                                if (last_match_pos != -1)
                                        gap = j - last_match_pos;

                                last_match_pos = j;

                                scal_match += 1.0f / ((float) gap);

                                if (scal_match > max_scal_match) {
                                        max_scal_match = scal_match;
                                        best_match_start = i;
                                        best_match_end = k;
                                        best_page_line = page_line;
                                        best_page_offset = page_offset;
```

```
                                        best_page = page;
                                    }
                                }

                                ++page_offset;
                            }
                        }

                        float ratio = max_scal_match / ((float) query_text.length());

                        if (ratio >= GOLDEN_RATIO) {
                            SearchResult result = new SearchResult ();
                            result.ratio = ratio;
                            result.offset = best_match_start;
                            result.length = best_match_end - best_match_start + 1;
                            result.text = text_0;
                            result.query_text = query_text_0;
                            result.page = best_page;
                            result.page_line = best_page_line;
                            result.page_offset = best_page_offset;
                            return result;
                        }

                        return null;
                    }
```

After successful presentation of the Java code, we would like to present the scalable window approach and its code.

Scalable window approach

The scalable window approach opposite to the naive method uses flowing window event when the mismatching occurs: in other words, it slowly checks for occurrences of match in the appearing window, thus the possible result of excess symbols in scrambled text is reduced. The sub-algorithm decides what symbol will be gap's left border, while the right border lays on the mismatched position [Y[1], Y[2]] (in pattern and scrambled text).

Example 1. Sample of scrambled text retrieved by Tesseract OCR

```
"дн     щ\n"
"У Х гасшрда Улш Моравия мемлекегйНЕ\n"
"цьшган мемлекег\n"
"мемлекетй\n"
"кен тараган славян таипалар в\n"
"Ь1с жерйнде Киев Русй аггьх\n"
```

This is to be better illustrated by the java code where the simple windowing algorithm is realized (code is below).

Java code for Scalable window approach:

```
public static SearchResult query (String text, String query_text, int cur_page) {
        if (text == null || query_text == null) return null;

        String text_0 = text;
```

```
		String query_text_0 = query_text;

		text = convert (text);
		query_text = removeSpaces (convert (query_text));

		if (query_text.length() <= MIN_LETTERS) return query_exact (text, query_text, text_0, query_text_0, cur_page);
		if (true) return query_large (text, query_text, text_0, query_text_0, cur_page);

	int pos_text = 0, pos_query = 0;
	int matched = 0;
	int last_match_pos = -1;
	int last_match_pos2 = -1;
	int max_matched = 0;
	int cons_match = 0;
	float scal_match = 0.0f;
	float max_scal_match = 0.0f;

	int start_match_pos = -1;
		int end_match_pos = -1;

		int best_pos_start = -1;
		int best_pos_end = -1;

		int last_pos_query = -1;

		int best_page = -1;
		int best_page_line = -1;
		int best_page_offset = -1;
		int page = 0;
		int page_line = 0;
		int page_offset = 0;


		int match_gap = MATCH_GAP;

		if (query_text.length() >= match_gap)
			match_gap = query_text.length() + 2;

		float max_ratio = 0;

	for (; pos_text < text.length() && pos_query < query_text.length(); ) {


	 char c1 = text.charAt(pos_text);
	   char c2 = query_text.charAt(pos_query);

	   if ((scal_match > max_scal_match) && matched > 1)
	   {
		max_scal_match = scal_match;
		best_pos_start = start_match_pos;
		best_pos_end = end_match_pos;
		best_page = page;
```

```
            best_page_line = page_line;
            best_page_offset = page_offset;
            max_matched = matched;
            max_ratio = (scal_match/((float)matched));
}

  if (c1 == c2) {
     int max_gap = 1;
     int a_gap = last_match_pos == -1 ? 0 : (pos_query - last_match_pos);
     int b_gap = last_match_pos2 == -1 ? 0 : (pos_text - last_match_pos2);
     int c_gap = a_gap > b_gap ? a_gap : b_gap;

     int p = 0;

     switch (cons_match) {
        case 1: max_gap = 2; break;
        case 2: max_gap = 3; break;
        case 3: max_gap = 4; break;
        default: if (cons_match > 3) max_gap = 5;
     }


     if (c_gap <= 1)
        ++cons_match;
     else
        cons_match = 0;

     if (c_gap == 0) c_gap = 1;
     if (c1 == c2) p = 1;

     if ((last_match_pos == -1 || a_gap <= max_gap)
           && (last_match_pos2 == -1 || b_gap <= max_gap)) {
        last_match_pos = pos_query;
        last_match_pos2 = pos_text;
        scal_match += ((float) p) / ((float)c_gap);
        matched += p;
        end_match_pos = pos_text;


     } else {

        if ((scal_match > max_scal_match) && matched > 1)
         {
                  max_scal_match = scal_match;
                  best_pos_start = start_match_pos;
                  best_pos_end = end_match_pos;
                  best_page = page;
                  best_page_line = page_line;
                  best_page_offset = page_offset;
                  max_matched = matched;
                  max_ratio = (scal_match/((float)matched));
         }
```

```
                matched = 1;
                cons_match = 1;
                scal_match = 1.0f;
                last_match_pos = -1;
                last_match_pos2 = -1;
                pos_text = -1;

                start_match_pos = -1;
                end_match_pos = -1;

                page = 0;
                page_line = 0;
                page_offset = 0;
                c1 = '\0';
            }

            if (start_match_pos == -1) {
                start_match_pos = pos_text;
                end_match_pos = pos_text;
            }

            if (c1 == '\n') {
                        page_line++;
                        page_offset = 0;
                } else if (((int) c1) == 12) {
                        ++page;
                        page_line = page_offset = 0;
                } else
                        ++page_offset;

            ++pos_text;
            ++pos_query;


        } else {
            boolean matched1 = false;
            for (int i = pos_query + 1; i < query_text.length() && (i < (pos_query +
match_gap)); ++i)
                if (c1 == query_text.charAt(i)) {
                    pos_query = i;
                    matched1 = true;
                    break;
                }
            if (!matched1) {
                int v_page = page;
                int v_page_line = page_line;
                int v_page_offset = page_offset;

                for (int i = pos_text + 1; i < text.length() && (i < (pos_text + match_gap)); ++i)
                {
                    if (c2 == text.charAt(i)) {
                            page = v_page;
```

```
                    page_line = v_page_line;
                    page_offset = v_page_offset;

                pos_text = i;
                matched1 = true;
                break;
              }

              if (text.charAt(i) == '\n') {
                    v_page_line++;
                    v_page_offset = 0;
             } else if (((int) text.charAt(i)) == 12) {
                    ++v_page;
                    v_page_line = v_page_offset = 0;
             } else
                    ++v_page_offset;
            }

            if (!matched1) {
               ++pos_query;

            }
        }


    }
}

if (pos_text == text.length()) {
   last_pos_query = pos_query;
} else {
   last_pos_query = -1;
}

if (text.length() == 0) return null;

if ((scal_match > max_scal_match) && matched > 1)
{
 max_scal_match = scal_match;
           best_pos_start = start_match_pos;
           best_pos_end = end_match_pos;
           best_page = page;
           best_page_line = page_line;
           best_page_offset = page_offset;
           max_matched = matched;
           max_ratio = scal_match/((float)matched);
 }

float retf = 0;
if (max_matched > 0)
 retf = Math.max(retf, (max_scal_match / ((float) max_matched)));
else
 retf = Math.max(retf, (max_scal_match / ((float)query_text.length())));
```

}

Obviously, the algorithm uses input parameters for windowing algorithm. This set can be extended according to the, for instance, textual model of the text. In this example the textual model is a scrambled text with excess symbols produced by the engine which are incorrect and are to be removed or replaced. Of course, the final reduction leads to the exact text extraction.

Now we are going for the application part, i.e the experimentation part. We have presented an Android Program, which was developed by authors, lunched by Google Inc.

Experimentation

Actually, the method described in this article were realized in the application, published by Google Inc. The program simply searches for extracted text in file system of the mobile device (Android program). Two different views are given for reference.

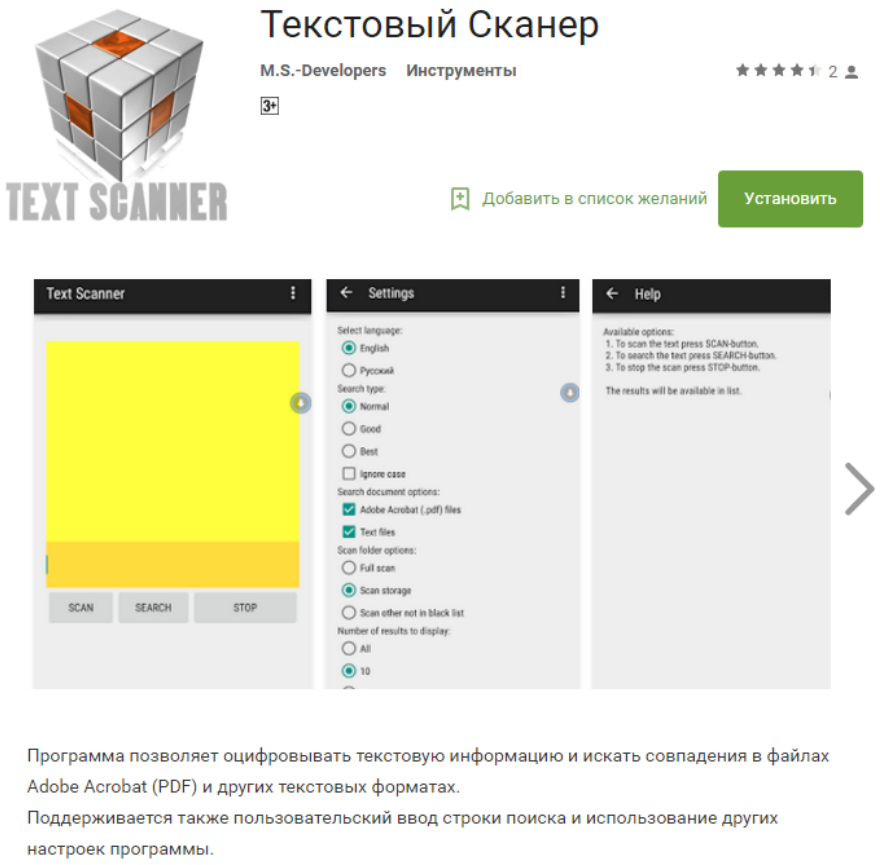

Figure 1 – The experimental program on Google Play

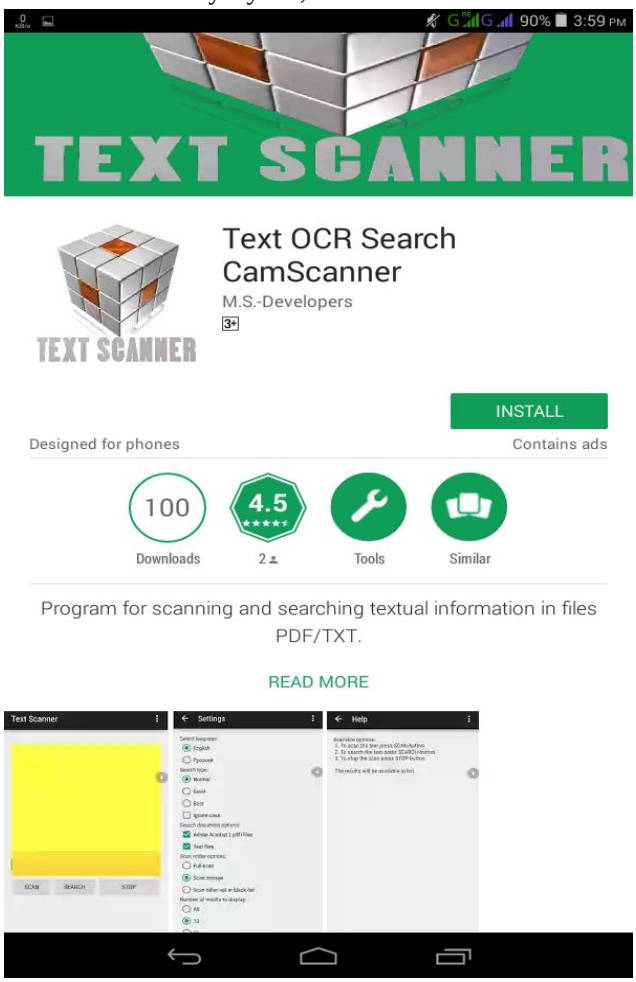

Figure 2 – A view of Android program on Google play store

Conclusion

So we have used the above algorithm for the extraction of text patterns. However the gap penalties as well as OCR engines were well studied in the past, for example, the problem of extracting the text pattern still remains open. This is mainly due to the complexity of the task when we need the fast pattern extractor on the partially extracted set of string data. So we think this paper gives a short development to this problem. And the interested researcher may put their focus on these issues.

Acknowledgements

Authors owe his special debt of gratitude towards his family members, for their keen interest and cooperation.

Funding

This project was partially supported by an educational grant of the Ministry of Education and Science of Republic Kazakhstan during 2006-2009.

References

[1] Régnier, Mireille. Knuth-Morris-Pratt algorithm: an analysis. International Symposium on Mathematical Foundations of Computer Science. Springer, Berlin, Heidelberg, 1989.

[2] Boyer, Robert S., and J. Strother Moore. A fast string searching algorithm. Communications of the ACM 20.10. 1977. 762-772.

[3] Prasetia, Yoga, Ghulam Asrofi Buntoro, and Dwiyono Ariyadi. Application of the Knuth-Morris-Pratt Algorithm on Android-based Money Recognition Applications for the Blind. Journal Teknik Informatika CIT Medicom. 2021. 13(2). 82-93.

[4] Wankhede, Poonam A., and Sudhir W. Mohod. A different image content-based retrievals using OCR techniques. IEEE Int. conf. of electronics, communication and aerospace technology (ICECA). 2017. 2.

[5] Hamming, Richard W. Error detecting and error correcting codes. The Bell system technical journal. 1950. 29(2). 147-160.

[6] Tesseract OCR, GitHub // https://github.com/tesseract-ocr (accessed Oct 11, 2021).

UDC004.02
IRSTI 20.53.15

MEMBERSHIP PROBLEM IN NON-DETERMINISTIC FINITE AUTOMATA FOR EXTENDED REGULAR EXPRESSIONS IN LINEAR POLYNOMIAL TIME

Mirzakhmet Syzdykov

al-Farabi Kazakh National University, Almaty, Kazakhstan
mspmail598@gmail.com
ORCID ID: https://orcid.org/0000-0002-8086-775X

Abstract. The recent work on implementing regular expression (RE) matching or membership problem solution for extended operators (ERE) like intersection, complement and subtraction gave exponential results on the size of input. As our previous result was focused on deterministic finite automata (DFA) for extended regular expressions, we present the new linear algorithm for ERE matching on non-deterministic finite automata (NFA) with the help of De Morgan's law to re-write the expression in exceptional order so that the conditional matching satisfies the correctness of the matching algorithm on NFA. We also prove that the proposed methodology is correct within the extensions of NFA like logical states as it was done before for DFA in the prior scientific work. We will also show how to implement these logical states in NFA using typical constructions like Thompson's. The proof of linear working time is also given which is obvious due to the re-writing rules for correct implementation. The important role of concatenation operator over extended constructions is also shown. The algorithm working time is O(m*n), where m is the size of expression and n is the size of matching word.

Keywords: regular expression, membership problem, extended operators, linear algorithm

Introduction

Regular expressions denoted by R are the grammar rules which are used to express the languages L(R). This is widely used and powerful tool for working with textual data and parsing. It's commonly used in such programming products like Java, Perl or C#, etc.

We will define the languages and regular expressions as follows with respect to the supported operators:

L(R) = { a: a in A }, where A is the alphabet and a is a single symbol in it;

L(R1 | R2) = { L(R1) + L(R2) } - union of two languages;

L(R1 * R2) = { L(R1) * L(R2) } - concatenation of two languages;

L(R*) = { eps, L(R), L(R * R) … L(R * R * … * R) } - Kleene closure or star operator, where "eps" stands for an empty word.

For the extended regular expressions we define the additional operators which give the possibility to operate on regular languages as if they would be the sets:

L(R1 & R2) = { L(R1) & L(R2) } - intersection of two languages defined by the expressions;

L(R1 – R2) = { L(R1) – L(R2) } - subtraction of two languages;

L(~R) = { ~L(R) } - complement operator which defines all the strings in dictionary which aren't matched by regular expression R.

For our purposes we use the re-writing for complement operator which can be defined by subtraction operator as:

$$L(\sim R) = A^* - L(R) \quad (1)$$

In Combinatorics for logical and set operations there's De Morgan's law which is defined as follows:

$$A \mid B = \sim(\sim A \,\&\, \sim B),$$
$$A \,\&\, B = \sim(\sim A \mid \sim B). \quad (2)$$

The law (2) is true even for sets which can be defined by regular expressions and thus can be applied for the purpose of re-writing gramatically the regular expressions. Further we will show that it's required in special cases when concatenation operator is used.

In the next section the review of the previous work is given with respect to the actually presented optimal results in this work.

Before we will define the membership problem for the word w and regular expression R as follows:

$$w \text{ in } L(R) \quad (3)$$

Past work

Rosu gives the exponential algorithm for extended operators – this is the best known result to the present time [1]. Our algorithm differs from the prior version for DFA with the same constructions [2]. Thompson constructions are linear to the size of regular expression and are used in our algorithm [3], this mainly doesn't limit the type of algorithm for NFA synthesis as we will prove further. Rabin and Scott provide us with the subset construction algorithm of converting NFA directly to DFA [4] – this is as stated before the previous result proposed by an author. Gelade and Neven give the exponential estimation of the size, in our case, of the states for extended operators [5]. The last work focuses on the state explosion during subset construction when we were building DFA from the NFA[6] – this is the main fact why there is the reason of building the linear NFA within the linear matching time for the membership problem.

The prior works [7, 8] were focused on the building of semantic rules for subset construction of DFA supporting the extended operators – this is necessary to note that in our NFA the same logical rules are applied.

The work [9] is important to use in the sense of past published work with respect to the extended operators.

Hsieh gives the product algorithm for construction of certain types of operator extensions in ERE [10] – it was shown that these product constructions are of exponential nature [7]. For practical reasons of product construction algorithm on intersection, complement and subtraction we use Møller's software [11]: for certain types of expressions like "(0*1*… | …) [&, &~] (1*0*… | …)" it demonstrates the exponential explosion of the number of states and transitions as well as DFA state explosion for expressions in form "(0|1)1(0|1)(0|1) … (0|1)".

The quadratic of the size of the word was recently developed [12], however, our algorithm works in linear time of the size of expression and word.

Preliminaries

For the preliminary section we will define the NFA as a tuple:

$$<A, S, s0, T, F>, \quad (4)$$

where A is an alphabet, S is a set of states, s0 is a starting state, T stands for transitions and F is a set of final states.

In the past work [2] we defined the special states by which we extended the definition of NFA (4) with the intersection and subtraction operator constructions as follows:

$$<A, S, s0, T, F, B(S)>, \quad (5)$$

where B(S) is the set of logical conditions to be satisfied during the matching process or subset construction.

We define the set B(S) for intersection and subtraction while the complement is given by re-writing rule (1):

$$B(S) = \{ (1 \mid 2): L(R1) \,\&\, L(R2); (1 \,\&\, \sim 2) : L(R1) - L(R2) \}, \quad (6)$$

where pair of number one and two stands for the flag conditions in the final implementation in order to the state become active and, thus, is to be included further in the stack during the matching process in general as opposed to the subset construction [2].

As we are finished with introduction, review of the past work and preliminary information it's time to present the algorithm with a proof.

Re-writing algorithm

Our algorithm for NFA construction is based upon the previous result [2], while the DFA

construction is omitted as mainly DFA are exponentially large for the predefined set of expressions due to the Kleene star closure. Thus, we use the same non-deterministic constructions.

Before the construction we have to give the notion to the re-writing rules which are used for concatenation operator of two regular expressions with the different operators like union and intersection: other operators like complement and subtraction are omitted because there is no need to re-write the rules according to De Morgan's law so that the matching process is correct within the typical matching algorithm which is linearly defined by the upper bound:

$$O(\text{NFA Matching}) = O(N*M), \quad (7)$$

where N is the size of the regular expression and M is the limit of input. We will show in proof section of the algorithm that this is not required.

We state that in order of concatenation the following conditions are to be met in order to satisfy the correctness of the construction of NFA for solving membership problem:

$$\begin{aligned} &\text{NFA}((R1 \mid R2) * (R3 \,\&\, R4)) = \\ &\text{NFA}(\sim(\sim R1 \,\&\, \sim R2) * (R3 \,\&\, R4)) = \\ &\text{NFA}((R1 \mid R2) * \sim(\sim R3 \mid \sim R4)), \end{aligned} \quad (8)$$

where NFA(~R) is defined according to re-writing rule (1).

The same is true for subtraction and complement:

$$\begin{aligned} &\text{NFA}((R1 \mid R2) * (R3 - R4)) = \text{NFA}(\sim(\sim R1 \,\&\, \sim R2) * (R3 - R4)), \\ &\text{NFA}((R1 \mid R2) * \sim R3) = \text{NFA}(\sim(\sim R1 \,\&\, \sim R2) * \sim R3). \end{aligned} \quad (9)$$

And finally for the last combination like intersection:

$$\begin{aligned} &\text{NFA}((R1 \,\&\, R2) * (R3 - R4)) = \text{NFA}(\sim(\sim R1 \mid \sim R2) * (R3 - R4)), \\ &\text{NFA}((R1 \,\&\, R2) * \sim R3) = \text{NFA}(\sim(\sim R1 \mid \sim R2) * \sim R3). \end{aligned} \quad (10)$$

Thus, we use the re-writings in (8)-(10) according to De Morgan's law – the linear size of complement from regular expression here plays an important role and gives us the possibility to safe the size of the built NFA which is linear to the size of regular expression. The NFA by itself is constructed according to Thompson's rules [3].

It's necessary to note that the methodology as to the previous works [2, 7, 8] is also applicable to the general case for NFA as the preliminary automaton to be converted to deterministic is of the same modeling approach as it's used in the typical matching algorithm for the solution of membership problem.

In the next section we will prove the correctness of re-writing algorithm for certain types of intersection operator conditions when the operators like union and intersection are put in the right order.

Proof

In this section we will provide the reader with the proof of the correctness of the re-writing rules for the concatenation of extended operator of intersection and union-operator which is far more typical.

Let's define the function T(R) as the degree of possibility of matching the regular expression R in NFA – this function gives us the possibility to observe the number of situations during which the concatenation matching is resumed.

Thus, T(R) is defined as follows for the specific case like concatenation of union and intersection which, in turn, is the only special case to be considered:

$$\begin{aligned} &T(R1 \mid R2) = 2, \\ &T(R1 \,\&\, R2) = 1. \end{aligned} \quad (11)$$

For the concatenation operator we define the correctness of the matching in membership problem as the state when logical conditions are satisfied for union and intersection as well – this can be written as:

$$T(R1 * R2): T(R1) <= T(R2) \quad (12)$$

As per our re-writing rules the necessary condition (12) is satisfied, thus the correctness of algorithm is proved. In general we can use empty string function [9] to compute the next node in abstract syntax tree when parsing regular expression, however, this can be omitted as we can

simply rewrite the union operator according to De Morgan's law.

Another proof is to be made for the logical states in NFA: as per non-deterministic case they are remained without changes and are to be addressed for the static matching process without closure evaluation [2].

Conclusion

Thus, we obtained the linear polynomial results by applying De Morgan's law in re-writing rules. This gives us opportunity to build NFA-based engines for extended regular expressions as they work optimally and aren't of perfect fit for other problems which are not omitted in the presented algorithm – we gain all the power of NFA in membership problem by matching.

The author lefts not opened questions upon the effective linear matching of extended operators in RE, however, there could be other open problems like implementation the specific features in the same time.

For the practical purposes we have also developed the Java version of regular expression engine based on the algorithm described in this article. This program can be obtained upon the request.

Acknowledgements

The author expresses gratitude to Dr. Steven Kearns for co-operation on finishing this project and giving important and valuable notions – without his support and interest it wouldn't be possible to obtain the highest results described in this work.

Funding

This work was partially supported by an educational grant of the Ministry of Education and Sciences of Republic Kazakhstan during author's work in 2006-2009 at the Institute of Problems in Informatics and Control.

References

[1] Roşu, Grigore. An effective algorithm for the membership problem for extended regular expressions. International Conference on Foundations of Software Science and Computational Structures. Springer, Berlin, Heidelberg, 2007.

[2] Syzdykov, Mirzakhmet. Deterministic automata for extended regular expressions. *Open Computer Science*. 2017. 7(1). 24-28.

[3] Thompson, Ken. Programming techniques: Regular expression search algorithm. *Communications of the ACM*. 1968. 11(6). 419-422.

[4] Rabin, Michael O., Dana Scott. Finite automata and their decision problems. *IBM journal of research and development*. 1959. 3(2). 114-125.

[5] Gelade, Wouter, and Frank Neven. Succinctness of the complement and intersection of regular expressions. *ACM Transactions on Computational Logic (TOCL)*. 2012. 13(1). 1-19.

[6] Yang, Yi-Hua E., and Viktor K. Prasanna. Space-time tradeoff in regular expression matching with semi-deterministic finite automata. Proceedings IEEE INFOCOM. IEEE, 2011.

[7] Syzdykov, Mirzakhmet. Algorithm to Generate DFA for AND-operator in Regular Expression. *International Journal of Computer Applications*. 2015. 975. 8887.

[8] Syzdykov, Mirzakhmet. Methodology to Produce Deterministic Automaton for Extended Operators in Regular Expression. *International Journal of Scientific & Engineering Research*. 2017. 8. 1497-1500.

[9] Berry, Gerard, and Ravi Sethi. From regular expressions to deterministic automata. Theoretical computer science. 1986. 48. 117-126.

[10] Hsieh, Samuel. Product Construction of Finite-State Machines. Proceedings of the World Congress on Engineering and Computation Science. 2010. 1. 141-143.

[11] Møller, Anders. Dk.brics.automaton – finite-state automata and regular expressions for Java. 2021. http://www.brics.dk/automaton/ (accessed August 22, 2021).

[12] Kupferman, Orna, and Sharon Zuhovitzky. An improved algorithm for the membership problem for extended regular expressions. International Symposium on Mathematical Foundations of Computer Science. Springer, Berlin, Heidelberg. 2002.

UDC 001.89
IRSTI 81.93.29

STUDY OF A DYNAMIC SUBSTITUTION BOX

N.A. Kapalova[1], A. Haumen[2]

[1,2]Institute of Information and Computational Technologies, Almaty, Kazakhstan
[1]kapalova@ipic.kz, [2]haumen.armanbek@gmail.com
[1]ORCID ID: https://orcid.org/0000-0001-9743-9981
[2]ORCID ID: https://orcid.org/0000-0002-1670-2520

Abstract. The paper examines a previously developed method for generating a dynamic substitutionbox. This method allows generating substitution boxes (S-boxes) that change depending on the values of some parameter obtained from the secret key of the algorithm. The generated S-boxes are resistant to linear and differential cryptanalysis, since they are random, not known in advance, and depend on the secret key. The obtained dynamic substitution boxes were examined for nonlinearity, and the results were compared with S-boxes of well-known symmetric block algorithms such as AES, Kuznyechik, SM4, BelT, and Kalyna.

Keywords: encryption algorithm, substitution box, dynamic S-box, nonlinear transformation.

Introduction

In the era of information technology development, symmetric block encryption algorithms are the main cryptographic means of ensuring confidentiality when processing information in modern information and telecommunication systems. Besides, block ciphers are used to ensure the integrity of information, and also as a basic element in the construction of other cryptographic primitives [1], such as pseudo-random sequence generators (PRNG), stream ciphers, and hash functions. The level of strength and properties of the symmetric block encryption algorithm used in a system to a significant extent determine the strength of the cryptographic protection of information, the security of cryptographic protocols, and the security of the information and telecommunications system as a whole.

What conditions must a strong block cipher satisfy? These conditions were formulated by C. Shannon in a number of his fundamental works on the theory of encryption [2]. A strong cipher must offerthe properties of diffusion and confusion:

1. Diffusion is a property of a cipher, when one character (bit) of the original text affects several characters (bits) of the ciphertext, optimally – all characters within one block. If this condition is met, then when encrypting two data blocks with minimal differences between them, completely different ciphertext blocks should be obtained. Exactly the same result should take place for the dependence of the ciphertext on the key – one character (bit) of the key must affect several characters (bits) of the ciphertext. Diffusion hides the relationship between the ciphertext and the original text.
2. Confusion is a property of a cipher to hide dependencies between characters in the original text and the ciphertext. If the cipher "mixes" the bits of the original text well enough, then the corresponding ciphertext does not contain any statistical and, moreover, functional regularities – again, for an outside observer with only limited computational resources. Confusion hides the relationship between the ciphertext and the key.

To meet the requirements for block ciphers, modern encryption algorithms use various transformations. This paper considers nonlinear transformations used in symmetric block encryption algorithms.

Nonlinear transformation in symmetric block encryption algorithms

A nonlinear transformation is required for every modern encryption algorithm and has been proven to be a strong cryptographic primitive against linear and differential cryptanalysis. Nonlinear

transformations in modern symmetric block algorithms are implemented in the form of substitution boxes (S-boxes) [3].

Considering that most modern block algorithms (Rijndael, Camellia, DES, etc.) use a single linear operation (modulo 2 addition) to introduce round keys and combine inter-round values, S-boxes are the only element that determines the nonlinearity of the encryption transformation and its level. resistance to cryptanalytic attacks. The number of rounds required to ensure the resistance of block ciphers to known types of cryptographic analysis is calculated based on the specified properties of nonlinear substitution nodes [4].

Many stream algorithms, cryptographic hash functions, and pseudo-random sequence generators are based on block ciphers or their structural elements. Thus, the cryptographic strength of most modern symmetric block algorithms largely depends on the properties of the selected S-boxes.

Despite the multi-modulus addition, the main nonlinear elements of modern ciphers are substitutions. Many different S-box criteria determine the strength of an encryption algorithm. However, today there is no unambiguous opinion about the need for most of them. Regardless of many existing solutions in the field of symmetric cryptography, the question of finding substitutions, the use of which in encryption algorithms provides protection against existing and promising types of attacks, remains relevant [4].

Substitutions used in cryptoalgorithmsshould meet the following criteria [5]:

a) Maximizingnonlinearity;
b) Theminimumdegreeis 3;
c) Minimizing the maximum value of the table of differentials.

In this paper, the properties of the nonlinearity of well-known encryption algorithms such as AES, Grasshopper, SM4, BelT, and others are considered, and the nonlinearity values of the S-boxes of these algorithms are calculated using a computer program. The program is implemented in Python 3.

Substitution boxes of known encryption algorithms

AES/Rijndael

Advanced Encryption Standard (AES), also known as a symmetric block cipher algorithm adopted as an encryption standard by the US government through an AES competition.

AES [7] is an encryption algorithm for 128-bit data blocks with keys of 128, 192, and 256 bits. AES is a simplified version of the Rijndael algorithm [8]. The original Rijndael algorithm differs in that it supports a wider set of block lengths.

The AES algorithm is widely used in cryptographic applications. In the AES algorithm, the SubBytes transformation is a nonlinear byte substitution performed independently with each byte [9]. The S-box substitution boxes are a fixed 8x256 bit table (Table 1). The nonlinear substitution operation is the main strength factor of this algorithm.

Table 1.

63, 7c, 77, 7b, f2, 6b, 6f, c5, 30, 01, 67, 2b, fe, d7, ab, 76, ca, 82, c9, 7d, fa, 59, 47, f0, ad, d4, a2, af, 9c, a4, 72, c0, b7, fd, 93, 26, 36, 3f, f7, cc, 34, a5, e5, f1, 71, d8, 31, 15, 04, c7, 23, c3, 18, 96, 05, 9a, 07, 12, 80, e2, eb, 27, b2, 75, 09, 83, 2c, 1a, 1b, 6e, 5a, a0, 52, 3b, d6, b3, 29, e3, 2f, 84, 53, d1, 00, ed, 20, fc, b1, 5b, 6a, cb, be, 39, 4a, 4c, 58, cf, d0, ef, aa, fb, 43, 4d, 33, 85, 45, f9, 02, 7f, 50, 3c, 9f, a8, 51, a3, 40, 8f, 92, 9d, 38, f5, bc, b6, da, 21, 10, ff, f3, d2, cd, 0c, 13, ec, 5f, 97, 44, 17, c4, a7, 7e, 3d, 64, 5d, 19, 73, 60, 81, 4f, dc, 22, 2a, 90, 88, 46, ee, b8, 17, de, 5e, 0b, db, e0, 32, 3a, 0a, 49, 06, 24, 5c, c2, d3, ac, 62, 91, 95, e4, 79, e7, c8, 37, 6d, 8d, d5, 4e, a9, 6c, 56, f4, ea, 65, 7a, ae, 08, ba, 78, 25, 2e, 1c, a6, b4, c6, e8, dd, 74, 1f, 4b, bd, 8b, 8a, 70, 3e, b5, 66, 48, 03, f6, 0e, 61, 35, 57, b9, 86, c1, 1d, 9e, e1, f8, 98, 11, 69, d9, 8e, 94, 9b, 1e, 87, e9, ce, 55, 28, df, 8c, a1, 89, 0d, bf, e6, 42, 68, 41, 99, 2d, 0f, b0, 54, bb, 16

Kuznyechik

Kuznyechik is a symmetric block cipher with a block size of 128 bits and a key length of 256

bits. The number of rounds is 10.

This cipher is approved as the standard GOST R 34.12-2015 RF [10]. The standard came into effect on January 1, 2016. The code was developed by the Center for Information Protection and Special Communications of the FSB of Russia with the participation of InfotecsOJSC.

The nonlinear transformation of the Kuznyechik algorithm is specified by the substitution S, which is a one-dimensional array of 256 bytes.

SM4

In January 2006, the SMS4 block cipher algorithm, developed by Professor Shu-Wang Lu, was declassified. This algorithm is used in China as the national standard for wireless local area networks. After the release of the GM / T 0002-2012 SM4 Block Cipher Algorithm standard on March 21, 2012, the algorithm was officially renamed SM4.

The block size of the SM4 encryption algorithm is 128 bits, the key size is also 128 bits. The number of rounds is 32 [11].

The nonlinear transformation is implemented by substitution $\boldsymbol{\tau}$, it is also specified in the form of a table of 8x256 bits.

BelT

BelT is the state standard for symmetric encryption and integrity control of the Republic of Belarus (STB 34.101.31-2007). Adopted as a preliminary standard in 2007. Introduced as the final standard in 2011.

The cipher has the block length of 128 bits and the key length of 256 bits.

Encryption is performed by eight rounds of transformations applied to the input block [12].

The nonlinear transformation of this algorithm is carried out through the substitution S. The substitution itself is specified in the form of a fixed table with the size of 8x256.

Kalyna

The Kalyna algorithm is a symmetric block cipher. It supports blocks of 128, 256, or 512 bits; the key length is equal to or doubled the block size.

Kalyna was adopted as the national encryption standard of Ukraine in 2015 (standard DSTU 7624: 2014) after the All-Ukrainian competition of cryptographers. The algorithm design is based on the Rijndael Algorithm (AES). The Kalyna algorithm retains all the basic operations of the Rijndael algorithm. The main differences are in the use of different S-boxes (4 different S-boxes are used), generated randomly, instead of identical S-boxes, and in the use of alternating addition with cyclic subkeys modulo 2 and modulo 2^{64} [13].

By means of a developed program, the values of the nonlinearity of the S-boxes of the above-considered encryption algorithms were calculated and analyzed.

Let$S = (f_0, f_1, \dots, f_{m-1})$be some$n \times m$ substitution, wheref_i is a Boolean function of$n$ variables. We denote byg_i the set of all linear combinations off_i. Thenthenonlinearity$S$is equal to [6]:

$$NL(S) = \min\left(NL(g_j)\right), 0 < j < 2^m$$

Table 2 below shows the results of calculating the value of the nonlinearity of the S-boxes.

Table 2.

Algorithms	Nonlinearityvalue
AES	112
Kuznyechik	116
SM4	112
BelT	110
Kalyna – S0	112
Kalyna – S1	110
Kalyna – S2	110
Kalyna – S3	112

Dynamic S-boxes

Recently, various scientific journals have published works on the creation of dynamic S-blocks of the encryption algorithm. In [3, 14, 15], methods of dynamic creation of S-boxes in various ways are considered. In [3], dynamic S-boxes are created based on the S-box of the AES algorithm. In [14], [15] S-boxes are generated dynamically using pseudo-random sequence generators.

In our work, we investigated one of the methods for creating dynamic S-boxes. Consider the developed method for generating S-boxes based on known and proven S-boxes. The idea behind this method is to generate dynamic S-boxes that modify with each change in the secret key. The main advantage of this approach is that S-boxes are random, key-dependent, and unknown in advance since both linear and differential cryptanalysis require known S-boxes.

The well-known S-box of the AES algorithm was chosen for the study. The values of this S-box are presented in Table 1. From the encryption master key, using various transformations, we obtain one byte, for example, by summing all the bytes of the master key modulo 2. The same byte will be used as a constant in the next affine transformation:

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{bmatrix} + \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \end{bmatrix}$$

where$a_i$arethebitsofthe S-boxbyte, $c_i$are the constant bits (the byte obtained from the master key), $b_i$are the bits of the new S-box byte

As a result of this affine transformation, we get a new S-box that differs from the original S-box. The resulting S-block will be used in the process of nonlinear transformation of the encryption algorithm

In the course of the study, it was revealed that after such a transformationpreserved the nonlinearity properties of the S-boxes. The experimental results are shown in Table 3.

Table 3.

Algorithm	Initialvalueofnonlinearity	Non-linearity value after transformation
AES	112	112
Kuznyechik	116	116
SM4	112	112
BelT	110	110
Kalyna-S0	112	112
Kalyna-S1	110	110
Kalyna-S2	110	110
Kalyna-S3	112	112

Also, various properties of dynamically generated S-boxes were investigated using special programs developed in our laboratory.

Table 4 shows the results of the study of the dynamic S-box of the AES algorithm, obtained with the value of C = 36, 109, and 221.

Next, we investigated various cryptographic properties of the created S-box. We consider a nonlinear node effective if it provides resistance to currently known cryptographic analysis methods.

In most of the well-known works in the field of analysis and synthesis of nonlinear substitution nodes of modern symmetric block ciphers, the mathematical apparatus of cryptographic Boolean functions is used [16]. Moreover, each S-box is represented by a set of component Boolean functions, the properties of which characterize the efficiency of the nonlinear substitutionnode. The following are used as the main criteria and performance indicators: balance and nonlinearity of component Boolean functions; correlation immunity; propagation criterion; algebraic degree; the value of the autocorrelation function.

Let us introduce the basic concepts and definitions used in what follows to assess the efficiency of nonlinear substitution nodes [16].

A Boolean function f of *n* variables is a function that maps from the field $GF(2^n)$ of all binary vectors $x = (x_1, \ldots, x_n)$ of length *n* into the field $GF(2)$. Boolean functions are usually represented in algebraic normal form. The field $GF(2^n)$ consist of 2^n vectors α_i: $\alpha_0 = (0,\ldots,0,0)$, $\alpha_1 = (0,\ldots,0,1)$,..., $\alpha_{2^n-1} = (1,\ldots,1,1)$, $\alpha_i \in V_n$, where V_n where V_n is a vector space in $GF(2^n)$.

The sequence of a function f is a (1,-1) sequence defined as $\left((-1)^{f(\alpha_0)}, (-1)^{f(\alpha_1)}, \ldots, (-1)^{f(\alpha_{2^n-1})}\right)$.

The truth table of a function f is a (0,1) sequence defined as $(f(\alpha_0), f(\alpha_1), \ldots, f(\alpha_{2^n-1}),)$.

The sequence of a function *f* is *balanced* if its (0,1) sequence ((1,-1) sequence) contains the same number of zeros and ones (ones and minus ones). A function *f* is balanced if its sequence is balanced.

Equivalent definition: A function *f* over $GF(2^n)$ is balanced if its outputs are equiprobable:

$$|\{x|f(x) = 0\}| = |\{x|f(x) = 1\}| = 2^{n-1}.$$

An affine function f is a function of the form $f = a_1x_1 \oplus \ldots \oplus a_nx_n \oplus c$, where a_j, $c \in GF(2)$, $j = 1, 2,\ldots, n$. A function *f* is called linear if $c = 0$.

The Hamming weight of the vector α, denoted as $W(\alpha)$, is the number of ones in the vector (sequence). *The Hamming distance d(f,g)* between the sequences of two functions *f* and *g* is the number of positions in which the sequences of these functions are different.

The nonlinearity of transformation (N_S) is the minimum Hamming distance between the output sequence *S* and all output sequences of affine functions over some field:

$$N_s = min\{d(S, j)\}, \text{ where j is the set of affine functions.}$$

The nonlinearity of a function (N_f) is the minimum Hamming distance N_f between the function *f* and all affine functions over $GF(2n)$:

$$N_f = min\{d(f, j)\}, \text{ where j is the set of affine functions.}$$

For an arbitrary function *f* the nonlinearity N_f over $GF(2^n)$ can reach:

$$N_f \leq 2^{n-1} - 2^{\frac{n}{2}-1}.$$

For a balanced function *f* over $GF(2^n)$ ($n \geq 3$) the nonlinearity N_f can reach:

$$N_f \leq \begin{cases} 2^{n-1} - 2^{\frac{n}{2}-1} - 2, n = 2k \\ \left[\!\left[2^{n-1} - 2^{\frac{n}{2}-1}\right]\!\right], n = 2k = 1 \end{cases}$$

where $\|x\|$ is the maximum even integer less than or equal to x.

A function *f* possesses *correlation immunity* of order *k* if the output sequence of the function $y \in Y$ is statistically independent of any subset of *k* input coordinates:

$$\forall\{x_1, \ldots x_k\} P(y \in Y/\{x_1, \ldots x_k\} \in X) = P(y \in Y).$$

Table 4.

Properties	S-box-1	S-box-2	S-box-3
ParameterCvalues	36	109	221
Hammingweight	128	128	128
Balance	True	True	True
Hammingweight - Minimum	128	128	128
Hammingdistance	128	128	128
Nonlinearity(min)	112	112	112
Nonlinearity(max)	144	144	144

Correlationvalue(min)	-32	-32	-32
Correlationvalue(max)	32	32	32
|AC| min	-32	-32	-32
|AC|max	32	32	32
| SSI |min	133120	133120	133120
| SSI |max	133120	133120	133120
SAC	False	False	False
Propagationcriterion	N/A	N/A	N/A
CI	N/A	N/A	N/A
t-stability	N/A	N/A	N/A

The resulting S-box will be used for encryption. Each encryption process will have its own S-box, the values of which are not known in advance. This property, in turn, complicates both differential and linear cryptanalysis. The decryption uses the inverse substitution box. The inverse S-box is also generated dynamically from the created main S-box. There is no need to store the inverse S-box.

Conclusion

Work in this area continues and the results obtained in the study will be used in the development of an encryption algorithm and research work that is being carried out at the Institute of Information and Computational Technologies of the Committee of Science of the Ministry of Education and Science of the Republic of Kazakhstan. Further, as a continuation of this work, other cryptographic properties of dynamically generated S-boxes will be investigated.

Acknowledgment

The research work was carried out within the framework of the project AP08856426 "Development and study of an encryption algorithm and the creation of a hardware and software complex for its implementation" at the Institute of Information and Computational Technologies.

References

[1] Gorbenko I.D., Dolgov V., Olejnikov R.V., Ruzhencev V.I., Mihajlenko M.S., Gorbenko YU.I., Razrabotka trebovanij i princip proektirovaniya perspektivnogo simmetrichnogo blochnogo algoritma shifrovaniya. *Izvestiya yuzhnogo federal'nogo universiteta. Tekhnicheskie nauki*. 2007. 76(1). 183-189. (in Russian)

[2] Shennon K. Raboty po teorii informacii i kibernetike, Moscow., IL, 1963, P.333-369. (in Russian)

[3] Kazlauskas K., Kazlauskas J., Key-dependent S-box generation in AES block cipher system. *Informatica*. 2009. 20. 23-34

[4] Olejnikov R.V., Kazimirov A.V. Vybor S-blokov dlya simmetrichnyh kriptograficheskih algoritmov na osnove analiza algebraicheskih svojstv. *Vesn. Hark. nac. un-tu. Ser. Matematichne modelyuvannya. informacijni tekhnologii*. Avtomatizovani sistemi upravlinnya, Kharkiv., 2010. 925. 79-86. (in Russian)

[5] Gorbenko I. D., Gorbenko YU. I. Prikladna kriptologiya,. - Kharkiv.: Fort, 2012. – 870 p. (in Russian)

[6] Kazimirov A.I. Metody i sredstva generacii nelinejnyh uzlov zameny dlya simmetrichnyh kriptoalgoritmov. Dissetraciya na soiskanie uchenoj stepeni kanditata tekhnicheskih nauk. Har'kovskij nacional'nyj universitet radioelektroniki. Kharkiv, 2013 (in Russian)

[7] Specification for the Advanced Encryption Standard (AES) [Electronic resource]. Available at: URL: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf. (Accessed 02.05.2021)

[8] Daemen J., Rijmen V. AES Proposal: Rijndael [Electronic resource]. Available at:– URL: http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf (Accessed 02.05.2021)

[9] Babenko L.K., Ishchukova E.A. Sovremennye algoritmy blochnogo shifrovaniya i metody ih analiza. – Moscow: Gelios APV, 2006. - 376 p. (in Russian)

[10] Kriptograficheskaya zashchita informacii Blochnye shifry -GOST R 34.12-2015 [Electronic resource]. Available at: – URL: https://tc26.ru/standard/gost/GOST_R_3412-2015.pdf (Accessed:

02.05.2021) (in Russian)

[11] SMS4 Encryption Algorithm for Wireless Networks. Translated and typeset by Whit field Diffie of Sun Microsystems and George Ledin of Sonoma State University, 15 May 2008

[12] Agievich S.V., Galinskij V.A., Mikulich N.D., Harin YU.S. Algoritm blochnogo shifrovaniya BelT / Upravlenie zashchitoj informacii, Vol. 6, №4, 2002. - P.407-412. (in Russian)

[13] Kuznecov O.O., Ivanenko D.V., Kolovanova E.P. Modelirovanie perspektivnogo blochnogo shifra «Kalina». *Prikladna radioelektronika: nauk.-tekhn. zhurnal*. 2014. 13(3). 201-207. (in Russian)

[14] Cassal-Quiroga B. B., Campos-Cantin E.. Generation of Dynamical S-Boxes for Block Ciphers via Extended Logistic Map. *Mathematical Problems in Engineering*. 2020. 2. 12. https://doi.org/10.1155/2020/2702653

[15] Jiqiang Lu, Hwajung Seo. A Key Selected S-Box Mechanism and Its Investigation in Modern Block Cipher Design, Security and Communication Networks, vol.2020, Article ID1457419, 26 pages, 2020. https://doi.org/10.1155/2020/1457419

[16] Kuznetsov A.A., Moskovchenko I.V., Prokopovich-Tkachenko D.I., Kuznetsova T.Yu.. Heuristic methods of gradient search for cryptographic Boolean functions. *Kharkiv National University of Radio Electronics, Radio engineering journal,* 2018. 195. 150-164.

Исследование динамической таблицы подстановок

Н.А.Капалова[1], **А.Хаумен**[1]
[1]Институт информационных и вычислительных технологий КН МОН
Алматы, Казахстан
e-mail: kapalova@ipic.kz, haumen.armanbek@gmail.com

Аннотация: В работе исследуется ранее разработанный метод генерации динамической таблицы подстановок. Данный метод позволяет генерировать таблицы подстановок (S-блоки), изменяющиеся в зависимости от значений некоторого параметра, получаемых из секретного ключа алгоритма. Генерируемые S-блоки устойчивы к линейному и дифференциальному криптоанализу, так как они являются случайными, заранее не известны и зависят от секретного ключа. Полученные динамические таблицы подстановок были исследованы на нелинейность, а результаты сравнивались с S-блоками известных симметричных блочных алгоритмов, таких как AES, Кузнечик, SM4, BelT и Калина.

Ключевые слова: алгоритм шифрования, таблица подстановок, динамический S-блок, нелинейное преобразование.

Динамикалық алмастыру кестелерін зерттеу

Н.А.Капалова[1], **А.Хаумен**[1]
[1]Ақпараттық және есептеуіш технологиялар институты, БжҒМ ҒК, Алматы, Қазақстан
e-mail: kapalova@ipic.kz, haumen.armanbek@gmail.com

Аннотация: Аталмыш жұмыста динамикалық алмастыру кестелерін жасаудың бұрынырақ құрастырылған тәсілі зерттелінеді. Бұл тәсіл құпия кілттен алынатын қандай да бір параметрдің мәніне байланысты өзгеріп отыратын динамикалық алмастыру кестелерін (S-блоктар) жасауға мүмкіндік береді. Құрастырылған S-блоктар сызықтық және дифференциалдық криптоталдауларға төтеп бере алады, себебі, алынған S-блоктар кездейсоқ, алдын ала белгісіз және олар құпия кілттерге тәуелді болмақ. Алынған динамикалық алмастыру кестелерінің сызықты емес болу қасиеті зерттелініп, нәтижелері AES, Кузнечик, SM4, BelT және Калина сияқты танымал симметриялы блоктық алгоритмдердің S-блоктарымен салыстырылып қарастырылды.

Түйін сөздер: шифрлеу алгоритмі, алмастыру кестесі, динамикалық S-блок, сызықты емес түрлендіру.

UDC 51-76; 004.11
IRSTI 50.37.23; 50.41.25

ОБРАБОТКА ГОЛОСОВОЙ ИНФОРМАЦИИ ДЛЯ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ

М.С. Әлиасқар[2], Т.Ж. Мазаков[1,2], Г.С. Байрбекова[1], Н.Т. Исимов[1], Т.С.Шорманов[2], Д.К. Мухаев[2]

[1]Институт информационных и вычислительных технологий КН МОН РК, Казахстан
[2]Казахский национальный университет имени аль-Фараби, Казахстан
87019931011@mail.ru
[2]ORCID ID: https://orcid.org/0000-0001-9345-5167

Abstract. Потребность в проверке личности людей с помощью надежных методов и параметров быстро возрастает во всем мире в эту информационную эпоху из-за желания сообщества выполнять повседневные процессы, такие как перевод денег или запрос услуги с использованием удаленных систем или колл-центров. Традиционные методы аутентификации, такие как использование паролей и показ удостоверений личности, теперь заменяются нашими физическими или поведенческими функциями, которые нельзя заменить или имитировать. Используя наши биометрические функции, методы аутентификации теперь могут выполняться только с использованием смартфонов, камер или только микрофона. Биометрические функции обеспечивают разные уровни шкалы доверительного интервала, у каждой из них есть свои плюсы и минусы, поэтому их можно выбрать по способности отвечать на запросы аутентификации, требующие разных уровней точности. Голосовая биометрия или технология распознавания говорящего обеспечивает эффективный и надежный способ аутентификации заявителя без необходимости находиться в одном и том же физическом месте и без особых усилий говорящего, более того, это можно сделать быстро во время телефонного звонка. Принимая во внимание рост числа мошеннических атак в последнее время из года в год и возможность его аутентификации, не сталкиваясь лицом к лицу с истцом, неудивительно, что использование технологии голосовой аутентификации растет в сфере банковских услуг и центров обработки вызовов. Это исследование представляет собой краткий обзор основных методов и исследований в области биометрии для личной идентификации.

Ключевые слова: биометрические технологии, голосовая аутентификация, извлечение голосовых характеристик, моделирование динамиков.

Введение

В современном мире все больше проявляется интерес к голосовым технологиям, в частности, к идентификации личности. Это объясняется, с одной стороны, появлением высокопроизводительных вычислительных систем на базе персональных компьютеров и аппаратных средств, позволяющих производить ввод сигнала в компьютер, а, с другой стороны, высокой потребностью систем аутентификации в разных областях.

Метод опознавания личности по голосу существует с тех пор, как человек научился говорить. Поэтому достоинства и недостатки этого метода известны всем. Как не всегда по ответу на вопрос «Кто там?» мы можем определить, что за дверью стоит знакомый человек, и приходится развеивать свои сомнения, заглянув в дверной глазок, так и техническая система идентификации может ошибаться в силу изменения голоса отдельного человека.

Привлекательность данного метода - удобство в применении. Метод проверки голоса имеет два положительных отличия от остальных биометрических методов. Во-первых, это идеальный способ для телекоммуникационных приложений. Во-вторых, большинство современных компьютеров уже имеют необходимое аппаратное обеспечение. Продукты с проверкой голоса сейчас предлагают банки и другие компаний.

Основная проблема, связанная с этим подходом, - точность идентификации. Однако это

не является серьезной проблемой с того момента, как устройства идентификации различают характеристики человеческой речи. Голос формируется из комбинации физиологических и поведенческих факторов.

Идентификация по голосу удобный, но в тоже время не такой надежный, как другие биометрические методы. Например, человек с простудой или ларингитом может испытывать трудности при использовании данных систем. Существует также возможность воспроизведения звукозаписи.

Методы исследования

Биометрическая система, по существу, распознает или извлекает шаблоны определенных физиологических или поведенческих характеристик, которыми обладает целевой человек, и использует эти шаблоны для сопоставления с заданными данными.

К настоящему моменту у нас и за рубежом реализованы системы автоматической идентификации по голосу, большинство из которых строятся по единой концептуальной схеме:

- производится регистрация пользователя и вычисляется шаблон;
- выбираются участки речевого потока для дальнейшего анализа;
- осуществляется первичная обработка сигнала;
- вычисляются первичные параметры;
- строится «отпечаток» (шаблон) голоса;
- производится сравнение «отпечатков» голосов и формируется решение по идентичности голосов или «близости» голоса к группе голосов [1].

Гипотетически биометрическая система состоит из двух основных модулей: регистрации и идентификации. Система сканирует особенности или, другими словами, биометрические характеристики человека с помощью биометрического датчика, получает цифровое представление этих функций и сохраняет его в качестве шаблона в центральной базе данных или на смарт-карте на этапе регистрации.

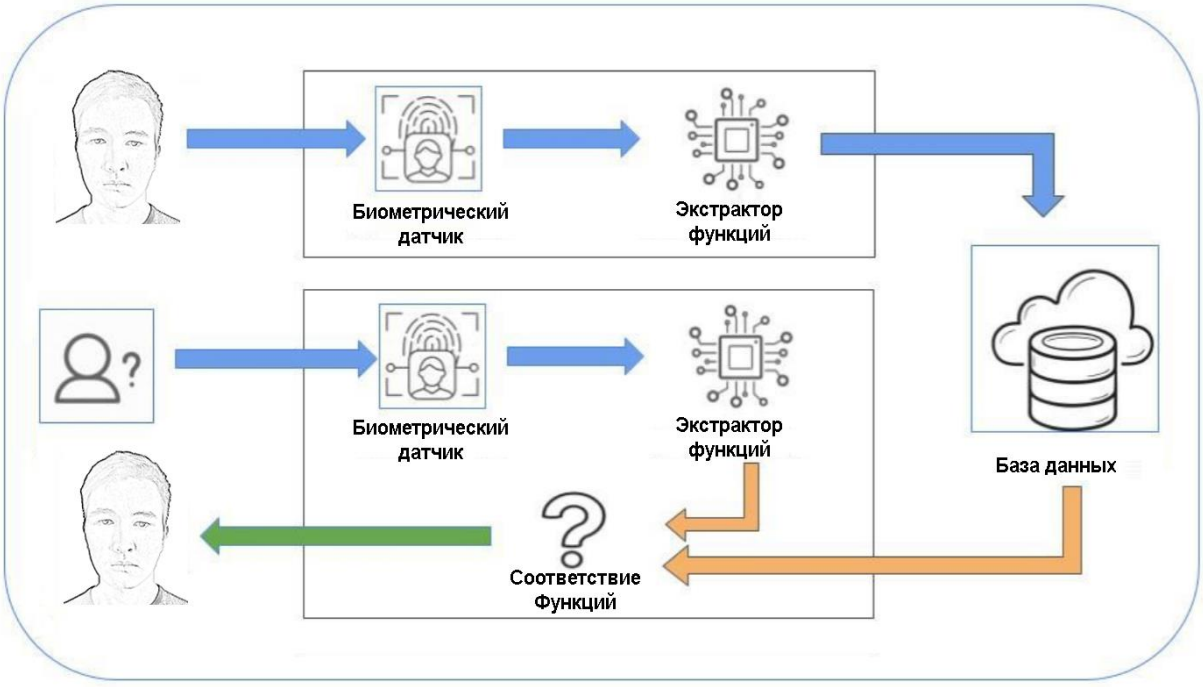

Рисунок 1 – Гипотетическая биометрическая система

Модуль распознавания снова сканирует биометрические характеристики целевого человека и преобразует их в цифровой формат, который используется на этапе регистрации. Затем система использует эти данные для сопоставления характеристик, что означает сравнение полученных данных с шаблонами для определения личности человека.

Общая производительность биометрической системы оценивается по ее показателю точности, скорости и хранению. Биометрические системы могут принять мошенника как действительного человека, и это называется «ложным совпадением» или, наоборот, система может отказать действительному лицу, и это называется «ложным несоответствием» [2].

Образец голоса – это индивидуальная характеристика, и невозможно найти двух людей с точно такой же спектрограммой. Спектрограмма – это визуальная запись речи, проанализированная по частоте, продолжительности и амплитуде. Поскольку голосовой отпечаток уникален для своего владельца, его можно использовать для уникальной идентификации.

Необходимое оборудование для голосовой аутентификации – это просто микрофон, поэтому его стоимость настолько мала, им легко пользоваться, и технология распознавания голоса сегодня присутствует в наших смартфонах. Но, конечно, он не идеален, как другие биометрические характеристики. Самый большой недостаток голоса в том, что он меняется в зависимости от возраста, и при переходе от детства к подростковому возрасту могут произойти резкие изменения. Также на голос могут негативно повлиять болезнь и мгновенные эмоции, акустика помещения и окружающий шум [3].

Голосовая аутентификация рассматривается как проблема распознавания образов, которая является ветвью машинного обучения. Основная задача при разработке системы голосовой аутентификации - извлечение речевого сигнала. Для извлечения речевых характеристик из речевого сигнала доступны некоторые методы. Модели динамиков создаются для отдельных лиц и сохраняются в виде голосовых баз данных после извлечения функций. Для создания моделей динамиков могут использоваться методы моделирования, включая векторное квантование (VQ), GMM (модели гауссовой смеси), HMM (скрытые марковские модели) и т.д.

Задача аутентификации говорящего состоит из двух компонентов: извлечения функций и сопоставления их, как упоминалось ранее. После извлечения уникальных характеристик из входной речи функции сравниваются с шаблонами выступающих, которые создаются с помощью различных методов моделирования и сохраняются [4].

Рисунок 2 – Блок-схема системы распознавания говорящих

Методы сопоставления функций используются как на этапе обучения, так и на этапе тестирования. Чтобы построить модель динамика, система обучается с использованием извлеченных функций на этапе обучения. Эта модель проверяется системой на этапе тестирования посредством распознавания выступающих.

Наиболее часто используемые методы построения моделей: векторное квантование (VQ), скрытая марковская модель (HMM) и модель гауссовой смеси (GMM) [5].

Векторное квантование (VQ): векторное квантование, пожалуй, самый простой алгоритм для сопоставления признаков и создания моделей с использованием векторов признаков. Тип VQ – это алгоритм обучения без учителя. Он создает кластеры, которые представляют модели зарегистрированных спикеров.

Во-первых, полученные векторы признаков классифицируются в разные кластеры. Кластеры включают в себя векторы признаков со схожими свойствами, и эти похожие векторы моделируют атрибуты говорящих. Сначала получаются векторы признаков, затем они сравниваются с центроидами уже существующих кластеров. Для этого используется расчет евклидова расстояния. Алгоритм помещает вектор признаков в кластер с минимальным расстоянием. После назначения вектора кластеру центроид кластера

обновляется. Другой термин для центроидов – это «кодовые слова», а термин «кодовая книга» используется для набора кодовых слов.

Скрытая марковская модель (HMM): HMM может моделировать статистические вариации характеристик, давать статистическое представление о том, как динамик воспроизводит звук [6]. Следовательно, HMM является более эффективным алгоритмом сопоставления признаков по сравнению с традиционной моделью VQ.

Модели HMM – это статистические модели, основанные на идее, которая является «распределением вероятностей состояния для времени x, условно независимого от всех предыдущих состояний, когда состояние во время x-1 задано. Кроме того, мы не можем напрямую определить состояния, для которых они невидимы. используйте или, другими словами, они «скрыты», но мы можем использовать параметры наблюдения для прогнозирования состояний. Цель состоит в том, чтобы определить эти скрытые значения состояния с помощью наблюдаемых параметров.

HMM - один из лучших методов анализа голоса, потому что он имеет четко определенную математическую структуру, не требует экспертных знаний о речевом сигнале, не накапливаются ошибки в анализе и не требует большого количества шаблонов.

Модель гауссовой смеси (GMM): модель гауссовой смеси - один из наиболее распространенных и успешных методов моделирования динамиков. Речевые атрибуты легко могут быть распределены по Гауссу, поэтому GMM - очень эффективный способ моделирования [7]. Плотность гауссовой смеси представляет собой взвешенную сумму M плотностей компонентов, где M представляет собой количество гауссианов. Каждого говорящего можно эффективно смоделировать и представить с помощью GMM, и на него ссылается модель, связанная с ним / ней.

Выводы

Биометрические – это общее название процессов, используемых для проверки и идентификации людей путем измерения их физиологических и поведенческих характеристик. Биометрические идентификаторы более надежны по сравнению с методами, основанными на знаниях и токенах, поскольку они обладают такими сильными характеристиками, как универсальность, уникальность, постоянство и возможность сбора. Наиболее часто используемые биометрические параметры – это отпечатки пальцев, геометрия руки, распознавание лиц, сетчатка, радужная оболочка глаза, голос, и каждая из них имеет свои плюсы и минусы по сравнению с другими.

Голосовая аутентификация может быть объяснена как распознавание говорящего с использованием информации, уникальной для человека. Системы распознавания громкоговорителей сначала извлекают из речевого сигнала определенные характеристики, а затем создают модели или шаблоны громкоговорителей для хранения этих функций. Наконец, система сравнивает голос, который должен быть аутентифицирован, с сохраненными шаблонами или голосовыми распечатками и пытается определить, совпадают ли они.

Системы голосовой аутентификации все чаще используют методы биометрии, потому что они не требуют никакого оборудования, кроме микрофона, взаимодействие пользователя не является обязательным и реализуется с помощью методов, основанных на сильной математической основе. Системы распознавания голоса, которые в настоящее время используются в таких областях, как судебная экспертиза и банковское дело.

Благодарность

Работа выполнена за счет средств программы целевого финансирования на основе договора по оказании услуг субподряда «Разработка национального электронного банка данных по научной зоологической коллекции Республики Казахстан, обеспечивающего их эффективное использование в науке и образовании».

References

[1] Singh N., Agrawal A., Khan R.A. Голосовая биометрия: технология аутентификации на основе голоса, передовая наука, инженерия и медицина. Июль 2018.

[2] Todkar S.P., Babar S.S., Ambike R.U., Suryakar P.B., Prasad J.R., Методы распознавания докладчиков. Материалы 3-ий Междунар. конф. по конвергенции в технологиях. 2018.

[3] Ahmad, K. S., Thosar, A. S., Nirmal, J. H., Pande, V. S. Уникальный подход к распознаванию говорящего независимо от текста с использованием наборов функций MFCC и вероятностной нейронной сети. Материалы 8-ой Междунар. конф. (ICAPR), 2015.

[4] Dehak N., Kenny P., Dehak R., Dumouchel P., Ouellet P., Front-end факторный анализ для проверки докладчика. IEEE Transactions on Audio, Speech, and Language Processing, 2011.

[5] Y. Lei, N. Scheffer, L. Ferrer, and M. McLaren. Новая схема распознавания говорящего с использованием фонетически осведомленной глубокой нейронной сети. Материалы Междунар.конф. по акустике, речи и обработке сигналов (ICASSP), 2014г.

[6] Bahmaninezhad F., Hansen J., Распознавание динамиков i-Vector / PLDA с использованием опорных векторов с дискриминантным анализом. Материалы Междунар. конф. IEEE по акустике, обработке речи и сигналов (ICASSP), 2017.

[7] Garcia-Romero D., McCree A., Анализ глубинных нейронных сетей для распознавания говорящего. Interspeech 2015.

УДК 531:536.66
МРНТИ 27.35.31: 30.19.25,27,29,51,55,57

РАСПРОСТРАНЕНИЕ ВОЛН ПОД ВОЗДЕЙСТВИЕМ ПОДВИЖНОЙ НАГРУЗКИ НА СЛОЕ ГРУНТА С ОСНОВАНИЕМ*

Айдосов Аллаярбек[1], Айдосов Галым Аллаярбекович[2],
Нарбаева Салтанат Муратбековна[3]

[1]РГП на ПВХ «Институт информационных и вычислительных технологий» КН МОН РК. г. Алматы, Казахстан, allayarbek@mail.ru
[2]КазМунайГаз Аймақ, г. Нур-Султан, Казахстан, galym.aidossov@gmail.com
[3] Казахский национальный университет им. аль-Фараби, г. Алматы, Казахстан, narbaevasalta777@gmail.com
[1]ORCID ID: https://orcid.org/0000-0003-2498-4035
[2]ORCID ID: https://orcid.org/0000-0001-6049-4346
[3]ORCID ID: https://orcid.org/0000-0001-5230-3781

Аннотация. Рассматривается задача разработки математических моделей волновое распределение с основанием под воздействием подвижной нагрузки в слое мягкого грунта.

Грунт моделируется идеальной нелинейно сжимаемый и необратимой разгрузкой средой, в которой зависимость между давлением и объемной деформацией при нагружении и в процессе разгрузки среды является линейной и необратимой.

Нагрузка приложена к верхней поверхности слоя и движется со сверх сейсмической скоростью. Рассматривается задача о воздействии подвижной нагрузки на двухслойную среду, состоящую из мягкого слоя грунта и упругоподатливой прокладки с разными толщинами и плотностями. Решение задачи построено аналитически как обратным, так прямым способами. В настоящей задаче срединная плоскость отсутствует. Поэтому в качестве искомых величин рассматривается смещения и деформации точек плоскости, которая при определённых условиях переходит в срединную плоскость слоя. При исследовании волновых процессов в деформируемых средах или при решении задач взаимодействия слоя с деформируемым основанием используются методы математической физики.

Ключевые слова: Математические модели, распространение, пластическая волна, аналитическое решение, фронт волны, идеальная жидкость, линейная сжимаемость, необратимая разгрузка. уравнение движение, неразрывность, состояния среды.

Введение

Анализ современного этапа развития механики выявлены, что в мире широко используется математические методы для проведенния научных исследований относящихся к теме. Практика выдвигает на передний план задачи многовариантных исследований двумерных и трехмерных систем, адекватное решение которых иногда возможно только путем математического моделирования. Как правило, найти замкнутое аналитическое решение для большинства проблем не представляется возможным, а экспериментальные исследования часто оказываются трудоемкими и опасными процессами [1].

Во второй половине 20-го века, относящие к 1950-1990 годы имеется множество работ, посвященных проблеме распространения волн в среде с деформируемом основанием. Анализ показывает, во-первых, что в большинстве этих работ исследования проводились для расчета линейных задач на прочность строительных конструкций с упругим основанием; во-вторых, в большинстве работ расчет элементов строительных конструкций рассматривался без влияния использования упруго-пластического основания. На основании анализа исследованных работ возникает потребность в разработке математические модели распространение волны на слое грунта со свойством нелинейно – сжимаемый и необратимой разгрузкой на упругом, упруго-пластическом и вязком основании с учетом

влияния температуры элементов конструкций и их основания [2]. Поэтому проблема, исследуемая в работе, учитывающая вышеперечисленные недостатки, является важной и актуальной.

Данная работа посвящена на постановке и разработке математической модели распространение волны в нелинейно – сжимаемой и необратимой разгрузкой полосе, лежащей на упругоподатливой основании. В качестве искомых величин рассматривается смещения и деформации точек плоскости, которая при определённых условиях переходит в срединную плоскость слоя [3]. При исследовании волновых процессов в деформируемых средах или при решении задач взаимодействия слоя с деформируемым основанием используются методы математической физики [4].

Анализ литературных данных и постановка проблемы

Иссдедованы ддинамические нагрузки возникающие в случаях, когда имеют место соударения частей работающих машин или их ударное действие на объекты производства (например, удар батана по нити в текстильных машинах, удары пневмо-молота по природе, в авиации и ракетной технике ими являются нерегулярно-циклические нагрузки, обусловленные действиями ударных волн и порывов ветра; в гражданском, промышленном, гидротехническом строительстве – сейсмические и всевозможные взрывные нагрузки; с последними часто приходится иметь дело в горных разработках и т.д. [5], [6].

Анализ исследовательских работ в данном направления в дальнем и ближнем зарубежья за последнее время по 2021 года показывают, что рассмотрены распространения волн в деформируемых слоистыхсредах под действием интенсивных нагрузок и проведены исследования в следующих направлениях [7,9-30]: экспериментальное исследование деформируемости, распространения ультразвуковых волн и акустической эмиссии каменной соли при трехосном сжатии; распространение естественных волн на многослойном вязкоупругом цилиндрическом теле, содержащем поверхность ослабленного механического контакта; моделирование распространения упругих волн при разведочном бурении на острове искусственного льда; вариационный принцип и распространение плоских волн в термоупругой среде с двойной пористостью по теории Лорда-Шульмана; влияние тепловых нагрузок на анализ распространения волн многомасштабных гибридных композитных балок; уединенные волны в деформируемых по степенях каналах с ламинарным или турбулентным потоком жидкости; анализ распространения волн интеллектуальных наноструктур; исследование распространения поперечных волн через параллельные стыки горных пород при напряжении на месте; влияние магнитного поля на термическое распространение акустических волн во вращающихся двухлучевых системах; математическое моделирование волны Стоунли в трансверсально-изотропной термоупругой среде; распространение косой поперечной волны в конечно деформируемых слоистых композитах; параметрическая оценка дисперсных вязкоупругих слоистых сред применительно к мониторингу состояния конструкций; пассивный контроль распространения трехмерных волн с помощью функционально градиентного слоя; теоретическая модель распространения акустической волны на мелководье; трехмерное моделирование влияния выпуклости на управление распространением нелинейных волн напряжений, вызванных взрывной нагрузкой; аналитическое исследование распространения волны Лява в функционально-градиентных средах с электродной границей и резко утолщенной несовершенной границей раздела; микроскопические неустойчивости и распространение упругих волн в конечно деформируемых слоистых материалах со сжимаемыми гиперупругими фазами; термомеханическое поведение многослойных сред на основе модели Лорда-Шульмана; распространение наклонных гравитационных волн во время внезапных стратосферных потеплений; распространение SH-волн в двух анизотропных слоях, связанных с

изотропным полупространством под действием силы тяжести; трехмерное численное моделирование горения метана и воздуха в инертных пористых средах в масштабе пор в условиях распространения волны горения в среде вверх и вниз по потоку; механизмы зарождения микротрещин в нержавеющей стали 316LN при синфазном термомеханическом усталостном нагружении; влияние мелких дефектов на усталостную прочность мартенситных нержавеющих сталей.

Все сказанное позволяет утверждать, что было целесообразным провести исследования по разработке математические модели напряженно-деформационного состояния материала с деформируемым основанием при динамической нагрузке.

Цель и задачи исследования

Целью данной работы является исследование, разработка математических моделей воздействия подвижной нагрузки на слой грунта конечной толщины, лежащей на горизонтальном упругоподатливой основании.

Грунт моделируется идеальной нелинейно – сжимаемый и необратимой разгрузкой средой, в

которой зависимость между давлением и объемной деформацией при нагружении и в процессе разгрузки среды является линейной и необратимой.

В рамках сформулированной цели ставятся и решаются следующие задачи:

– разработка математической модели распространение волны в нелинейно – сжимаемой и необратимой разгрузкой полосе, лежащей на упругоподатливой основании.

Материалы и методы исследований

Для решения исследовательских задач применяются методы математической физики с использованием законы сохранения количества движения, энергии, неразрывности, массы, начальные и граничные условия, разработка математической модели воздействия подвижной нагрузки на слой грунта конечной толщины, лежащей на горизонтальном упругоподатливой основании и разработка математической модели распространение волны в нелинейно – сжимаемой и необратимой разгрузкой полосе, лежащей на упругоподатливой основании

При решении волновых задач для деформируемых сред, описываемых уравнениями движения или для вязкоупругих сред, или при решении задач упругих (вязкоупругих) тело, поведения которых описывается уравнениями в частных производных четвертого или более высокого порядка. построения общих решений уравнений движения представляет трудную математическую задачу, причем эта сложность усугубляется различного вида граничными условиями. Нами получены решение задачи на основе классической приближенной теории воздействия подвижной нагрузки на слой грунта конечной толщины с деформируемым основанием.

Результаты исследований

Постановка и решение задачи разработка математической модели распространение волны в нелинейно – сжимаемой и необратимой разгрузкой полосе, лежащей на упругоподатливой основании. Рассматривается плоская задача о распространении пластической волны в двухслойной среде с плоскопараллельной границей раздела при воздействии интенсивной нагрузки спадающего профиля, перемещающейся вдоль ее верхней границы с постоянной сверх сейсмической скоростью D.

Двухслойная среда состоит из мягкого слоя грунта толщиной h с упруго-податливым деформируемым основанием. Грунт моделируется неупругой идеальной средой с линейной сжимаемостью и линейной необратимой разгрузкой. Следовательно, сопротивлением среды к сдвиговым усилиям пренебрегается.

Согласно данной постановке исследовано влияние деформируемости основания и

профиля нагрузки на распределение динамических параметров слоя и контактной поверхности. Сравниваются результаты числового расчета с результатами акустического слоя и слоя жестким основанием. Решение задачи построено в рядах, доказана их сходимость.

Пусть по верхней границе слоя с упругим основанием движется монотонно убывающая нормальная нагрузка со скоростью *D*, превосходящая скорость распространения волн. Материал слоя обладает таким свойством, что при нагружении и разгрузке связь между давлением P и объемной деформацией ε линейна и необратима, угол наклона E_2 ветви разгрузки диаграммы $P \sim \varepsilon$ превышает угол наклона E_1 ветви нагружении, т.е. $E_1 < E_2$.

Под действием вышеуказанной нагрузки в слое сначала распространяется волна сжатия Σ_1, которая достигается контактной линии сред побуждает в слое отраженную пластическую волну Σ_2, а во второй среде систему упругих (продольной и поперечной) волн Σ_a и Σ_b. При $E_1 < E_2$ скорость распространения характеристики $АД$ больше, чем скорость фронта Σ_2, следовательно, как в предыдущем разделе, возникают области 2, 3, 4, и т.д. На системе Σ_a и Σ_b материал слоя мгновенно нагружается, а затем областях 1, 2, 3, среда разгружается. Учитывая, что решение задачи в областях 1 и 2 было получено, ниже предлагается решение задачи только в областях 3 слоя и a, b упругой полуплоскости. Для совместной задачи области 3, a, b имеет место $f_2'\left(\frac{(1+\mu tg\alpha)}{tg\alpha}h\right) = \frac{P_0}{\rho_0 D}\sum_{n=1}^{\infty}\lambda^{-\lambda^{n+1}\frac{(1+\mu tg\alpha)}{tg\alpha}}$ и уравнения для потенциалов перемещения Φ, $\bar{\Psi}$ упругой полуплоскости[1-6]

$$\mu_1^2\frac{\partial^2\Phi}{\partial\xi^2} = \frac{\partial^2\Phi}{\partial\eta^2}, \quad \mu_2^2\frac{\partial^2\Psi}{\partial\xi^2} = \frac{\partial^2\Psi}{\partial\eta^2}, \tag{1}$$

$$\mu_1^2 = \left(\frac{D}{a_0}\right) - 1, \quad \mu_2^2 = \left(\frac{D}{b_0}\right) - 1, \quad a_0^2 = \frac{\lambda + 2G}{\rho_0}, \quad b_0^2 = \frac{G}{\rho_0}.$$

и по формуле Даламбера их решения представляется в виде

$$\varphi(\xi,\eta) = f_3(\xi - \mu\eta) + f_4(\xi + \mu\eta), \quad \Phi(\xi,\eta) = F_3(\xi - \mu_1\eta), \quad \Psi(\xi,\eta) = F_2(\xi - \mu_2\eta). \tag{2}$$

где ρ_{02}, λ, G – начальная плотность и коэффициенты Ламе упругой среды.

Граничные условия данной задачи следующие:

на фронте отраженной волны при $\eta + \xi tg\alpha = 2h$

$$tg\alpha\left(\vartheta_3^* - \vartheta_2^*\right) = u_3^* - u_2^*, \tag{3}$$

на контакте *AE* двух сред при $\eta = h, \quad \xi \geq \frac{h}{tg\alpha}$

$$\sigma_{\xi\eta} = 0, \quad D\left(\frac{\partial^2\Phi}{\partial\xi\partial\eta} + \frac{\partial^2\Psi}{\partial\xi^2}\right) = \frac{\partial\varphi}{\partial\xi}, \quad P = -\sigma_{\eta\eta}. \tag{4}$$

Здесь $\sigma_{\xi\eta}, \sigma_{\eta\eta}$ – компоненты напряжения в упругой среде. Для нахождения функции $f_4'(t)$ из (3) и (4) с учетом (2) получаем функциональное уравнение[1,5-10]

$$f_4'(\xi) - \lambda_1 f_4'(\lambda_0\xi + 2\mu h) = -\frac{\lambda_1}{\lambda_0}G_1(\xi), \tag{5}$$

где

$$G_1(\xi) = f_1'(\xi - 2\mu h) + \lambda_0 f_2'(\lambda_0 \xi + 2\mu h),$$

$$A(\lambda, G) = -\left[\lambda \frac{(\mu_1^2 + 1)(\mu_2^2 - 1)}{2\mu_1} + 2G\left(\frac{\mu_1(\mu_2^2 - 1)}{2} + \mu_2 \right) \right],$$

$$\frac{\lambda_1}{\lambda_2} = -\frac{A(\lambda, G) + \frac{\rho_0 D^2}{\mu}\left(1 + \frac{\mu_2^2 - 1}{2}\right)}{A(\lambda, G) - \frac{\rho_0 D^2}{\mu}\left(1 + \frac{\mu_2^2 - 1}{2}\right)}.$$

Решение уравнения (5) построено методом последовательных приближений. В самом деле, принимая за нулевое приближение

$$f_{40}'(\xi) = -\frac{\lambda_1}{\lambda_0} G_1(\xi).$$

для первого приближения имеем

$$f_{40}'(\xi) = -\frac{\lambda_1}{\lambda_0}\left[G_1(\xi) + \lambda_1 G_1(\lambda_0 \xi + 2\mu h) \right].$$

Тогда, продолжая процесс итерации, получим рекуррентную формулу вида

$$f_4'(\xi) = -\frac{\lambda_1}{\lambda_0}\left[G_1(\xi) + \sum_{n=1}^{\infty} \lambda_1^n G\left(\lambda_0^n \xi + 2\mu h \frac{(\lambda_0^n - 1)}{(\lambda_0 - 1)} \right) \right]. \quad (6)$$

Исследование показало, что $\lambda_1 << 1, \lambda_0 < 1$ и $G_1(\xi)$ монотонно убывающая функция.

Следовательно, по признаку Даламбера ряд (6) абсолютно сходится, и можно установить радиус его сходимости. Тогда решение задачи с учетом (6) примет вид [2-5]

$$P(\xi, \eta) = -\rho_0 D \Psi_{28}(\xi, \eta), \quad (7)$$

$$\vartheta(\xi, \eta) = -\mu \Psi_{29}(\xi, \eta). \quad (8)$$

где

$$\Psi_{28}(\xi, \eta) = \left\{ \begin{array}{l} G_1(\xi - \mu\eta + 2\mu h) - \frac{\lambda_1}{\lambda_0} G_1(\xi + \mu\eta) + \\ + \sum_{n=1}^{\infty} \lambda_1^n G_1\left[\lambda_0^n (\xi - \mu\eta + 2\mu h) + 2\mu h \frac{(\lambda_0^n - 1)}{(\lambda_0 - 1)} \right] - \\ - \frac{\lambda_1}{\lambda_0} \sum_{n=1}^{\infty} \lambda_1^n G_1\left[\lambda_0^n (\xi + \mu\eta) + 2\mu h \frac{(\lambda_0^n - 1)}{(\lambda_0 - 1)} \right] \end{array} \right\},$$

$$\Psi_{29}(\xi,\eta)=\left\{\begin{array}{l} G_1(\xi-\mu\eta+2\mu h)-\dfrac{\lambda_1}{\lambda_0}G_1(\xi+\mu\eta)+ \\ +\sum\limits_{n=1}^{\infty}\lambda_1^n G_1\left[\lambda_0^n(\xi-\mu\eta+2\mu h)+2\mu h\dfrac{(\lambda_9^n-1)}{(\lambda_0-1)}\right]+ \\ +\dfrac{\lambda_1}{\lambda_0}\sum\limits_{n=1}^{\infty}\lambda_1^n G_1\left[\lambda_0^n(\xi+\mu\eta)+2\mu h\dfrac{(\lambda_0^n-1)}{(\lambda_0-1)}\right] \end{array}\right\}.$$

В этом случае нормальной напряжения $\sigma_{\eta\eta}$ упругой полуплоскости в областях a и b определяется формулами

$$\sigma_{\eta\eta}=\frac{\mu\left(\mu_2^2-1\right)\left(1+\dfrac{\lambda_1}{\lambda_0}\right)}{2D\mu_1\left(1+\dfrac{\mu_2^2-1}{2}\right)}\Psi_{30}(\xi,\eta)+\frac{2G\mu_2\mu\left(1+\dfrac{\lambda_1}{\lambda_0}\right)}{D\left(1+\dfrac{\mu_2^2-1}{2}\right)}\Psi_{31}(\xi,\eta), \quad (9)$$

при $\xi-\mu_2\eta\ge 0, \quad \eta\ge h.$

$$\sigma_{\eta\eta}=\frac{\mu\left(\mu_2^2-1\right)\left(1+\dfrac{\lambda_1}{\lambda_0}\right)}{2D\mu_1\left(1+\dfrac{\mu_2^2-1}{2}\right)}\Psi_{32}(\xi,\eta), \quad (10)$$

при $\xi-\mu_2\eta\ge 0, \quad \mu=h$,

$$\Psi_{30}(\xi,\eta)=\left\{\begin{array}{l} \left[\lambda\left(\mu_2^2+1\right)+2G\mu_1^2\right]G_1\left[\left(\xi-\mu_1^2\eta\right)+\left(\mu_1+\mu\right)h\right]+ \\ +\sum\limits_{n=1}^{\infty}\lambda_0^n G_1\left[\lambda_0^n\left(\xi-\mu_1\eta+\left(\mu_1+\mu\right)h\right)+2\mu h\dfrac{(\lambda_0^n-1)}{(\lambda_0-1)}\right] \end{array}\right\},$$

$$\Psi_{31}(\xi,\eta)=\left\{\begin{array}{l} G_1\left[\left(\xi-\mu_2^2\eta\right)+\left(\mu_2+\mu\right)h\right]+ \\ +\sum\limits_{n=1}^{\infty}\lambda_1^n G_1\left[\lambda_0^n\left(\left(\xi-\mu_2\eta\right)+\left(\mu_2+\mu\right)h\right)+2\mu h\dfrac{(\lambda_0^n-1)}{(\lambda_0-1)}\right] \end{array}\right\},$$

$$\Psi_{32}(\xi,\eta)=\left\{\begin{array}{l} \left[\lambda\left(\mu_1^2+1\right)+2G\mu_1^2\right]G_1\left[\left(\xi-\mu_1\eta\right)+\left(\mu_1+\mu\right)h\right]+ \\ +\sum\limits_{n=1}^{\infty}\lambda_1^n G_1\left[\lambda_0^n\left(\xi-\mu_1\eta+\left(\mu_1+\mu\right)h\right)+2\mu h\dfrac{(\lambda_0^n-1)}{(\lambda_0-1)}\right] \end{array}\right\},.$$

Если $\lambda\to\infty, \quad G\to\infty,$ то $\lambda_1=-\lambda_0$, и из (2), (3) для случая слоя с абсолютно жестким основанием имеем

$$P(\xi,\eta)=-\rho_0 D\Psi_{33}(\xi,\eta), \quad (11)$$

$$\vartheta(\xi,\eta)=-\mu\Psi_{34}(\xi,\eta). \quad (12)$$

где

$$\Psi_{33}(\xi,\eta)=\left\{\begin{array}{l} G_1(\xi-\mu\eta+2\mu h)-G_1(\xi-\mu_1\eta)+ \\ +\sum_{n=1}^{\infty}(-\lambda_0)^n G_1\left[\lambda_0^n(\xi-\mu\eta+2\mu h)+2\mu h\frac{(\lambda_0^n-1)}{(\lambda_0-1)}\right]+ \\ +\sum_{n=1}^{\infty}(-\lambda_0)^n G_1\left[\lambda_0^n(\xi+\mu\eta)+2\mu h\frac{(\lambda_0^n-1)}{(\lambda_0-1)}\right]+ \end{array}\right\},$$

$$\Psi_{34}(\xi,\eta)=\left\{\begin{array}{l} G_1\left[(\xi-\mu\eta+2\mu h)-G_1(\xi+\mu\eta)\right]+ \\ +\sum_{n=1}^{\infty}(-\lambda_0)^n G_1\left[\lambda_0^n(\xi-\mu\eta+2\mu h)+2\mu h\frac{(\lambda_0^n-1)}{(\lambda_0-1)}\right]- \\ -\sum_{n=1}^{\infty}(-\lambda_0)^n G_1\left[\lambda_0^n(\xi+\mu\eta)+2\mu h\frac{(\lambda_0^n-1)}{(\lambda_0-1)}\right] \end{array}\right\},.$$

В дальнейшем на основе формулы (2) – (12) необходимо провести некоторые расчеты на ПК и проанализировать их.

Отметим, что вышеизложенная методика позволяет решить задачу о воздействии подвижной нагрузки на нелинейно – сжимаемую полосу, лежащей на упругом полупространстве.

Давление P своего максимального значения достигает при $\eta=h$ на линии AE является более или менее интенсивной. При затухание давления на глубине слоя происходит быстрее, чем при $\gamma=1$. Кроме того, с усилием жесткости основания происходит увеличение (уменьшение) величин давления (вертикальной составляющей скорости) на линии раздела сред. Изменение P и ϑ акустического слоя на $\eta=h$ происходит на линейному закону, и в данном случае, по сравнению с пластическим слоем, максимальные значения скорости ϑ и давления P получаются наибольшими. Однако наивысшее значение давление приобретает в случае акустического слоя, лежащего на жестком основании. Таким образом, учет деформативности основания снижает уровень давления, как на контактной поверхности, так и в слое. Также заметим, что при $\eta=h$ акустический слой на упругом основании получает наибольшую вертикальную скорость. На линии $\eta=\frac{2}{3}h$ параметры P и ϑ при $\gamma=1$ приобретают сравнительно большие значения и в зависимости от ξ имеют затухающий характер.

Обсуждение результатов исследования, постановка и решение задачи разработка математической модели распространение волны в нелинейно – сжимаемой и необратимой разгрузкой полосе, лежащей на упругоподатливой основании.

В исследовании сделана постанока задач, разработка математической модели воздействия подвижной нагрузки на слой грунта конечной толщины, лежащей на горизонтальном упругоподатливой основании и разработка математической модели распространение волны в нелинейно – сжимаемой и необратимой разгрузкой полосе, лежащей на упругоподатливой основании.. Таким образом, точная трехмерная задача движения вязкоупругого слоя переменной толщины, лежащей на деформируемом пористом водонасыщенном грунте, сводится к решению интегро-дифференциальных уравнений движения в потенциалах Φ_0, Φ_1, Φ_2 и $\bar{\Psi}_0$, $\bar{\Psi}_1$, $\bar{\Psi}_2$, при граничных условиях, при сформулированных ограничениях и нулевых начальных условиях.

Рассматривается задача о распространении пластической волны в двухслойной среде с

плоско параллельной границей раздела при воздействии интенсивной нагрузки спадающего профиля, перемещающейся вдоль ее верхней границы с постоянной сверх сейсмической скоростью *D*.

Двухслойная среда состоит из мягкого слоя грунта толщиной h с упругим деформируемым основанием. Грунт моделируется неупругой идеальной средой с линейной сжимаемостью и линейной необратимой разгрузкой. Следовательно, сопротивлением среды к сдвиговым усилиям пренебрегается. Согласно данной постановке исследовано влияние деформируемости основания и профиля нагрузки на распределение динамических параметров слоя и контактной поверхности. Пусть по верхней границе слоя с упругим основанием движется монотонно убывающая нормальная нагрузка со скоростью *D*, превосходящая скорость распространения волн не меняется, а материал слоя обладает таким свойством, что нагружении и разгрузке связь между давлением P и объемной деформацией ε линейна и необратима, угол наклона E_2 ветви разгрузки диаграммы $P \sim \varepsilon$ превышает угол наклона E_1 ветви нагружении, т.е. $E_1 < E_2$

По результатам исследования распространения волн в многослойном, в частности неоднородном, полупространстве с учетом необратимых процессов в рамках идеальной нелинейно-сжимаемой и линейно-упругой среды можно сделать следующие выводы:

Исследована задача о распространении пластической волны в двухслойной среде с плотностями ρ_1, ρ_2 для случая когда, диаграмма состояния $P = P(\varepsilon)$ первой среды (грунта) является ударной и при нагружении имеет вид $P(\varepsilon) = \alpha_1\varepsilon + \alpha_2\varepsilon^2$, а второй среды (черной породы скалы или прокладки) - упругой или жесткопластической. Задача решается аналитически как прямым, так и обратным методом с учетом волновых процессов во второй среде и без их учета. Анализ результатов, что при $\rho_1 > \rho_2$ учет упруго – пластических свойств второй среды (прокладки), моделируемой полупространством, приводит, в основном, к уменьшению максимальных значений напряжений (давления) на контакте двух сред. При $\rho_1 < \rho_2$ на контактной поверхности появляется концентрация напряжений и давление получает наибольшее значение в случае акустического слоя, лежащего на жестком основании. Качественная и количественная картина изменения величин давления и кинематических параметров зависит не только от жесткостных характеристик сред, но и от отношения их плотностей.

Грунт моделируется неупругой идеальной средой с линейной сжимаемостью и линейной необратимой разгрузкой. Следовательно, сопротивлением среды к сдвиговым усилиям пренебрегается. Согласно данной постановке исследовано влияние деформируемости основания и профиля нагрузки на распределение динамических параметров слоя и контактной поверхности. Сравниваются результаты числового расчета с результатами акустического слоя и слоя жестким основанием. Решение задачи построено в рядах, доказана их сходимость. Рассмотрена задача, когда по верхней границе слоя с основанием движется монотонно убывающая нормальная нагрузка со скоростью *D*, превосходящая скорость распространения волн не меняется, а материал слоя обладает таким свойством, что нагружении и разгрузке связь между давлением P и объемной деформацией ε линейна и необратима, угол наклона E_2 ветви разгрузки диаграммы $P \sim \varepsilon$ превышает угол наклона E_1 ветви нагружении, т.е. $E_1 < E_2$

Таким образом, выше проведенные исследования по изучению двумерного напряженно-деформированного состояния однородной, неоднородной и слоистой среды при интенсивном воздействии подвижной нагрузки на границу многослойного полупространства подтверждают необходимость и важность учета нелинейных, необратимых, волновых процессов.

Заключение

Построено математические модели распространение волны под воздействием подвижный нагрузки на нелинейно – сжимаемый и необратимой разгрузкой слой грунта, с основанием. Получены аналитическое решение задачи о распространении пластической волны в случае, когда зависимость между давлением и объемной деформацией при нагружении и разгрузке является линейной, но различной. На основе анализа результатов расчета показано, что если действующая на границе подвижная нагрузка имеет монотонно - убывающий профиль, то в области возмущения происходит разгрузка среды и косая волна сжатия получается волной нагрузки- разгрузки. Давление среды на фоне этой волны в зависимости от глубины спадает медленно, чем на свободной поверхности. В случае, когда зависимость между P и объемной деформацией ε при нагружении среды принимается нелинейной и ударной, что соответствует распространению в среде ударной волны, давление в области возмущения, по сравнению с линейным случаем, несколько завышается.

В качестве слоистой среды принимается мягкий слой грунта, моделируемый пластической полосой и упругое полупространства различных вариантах. В данной задаче упругим полупространством могут служить как горные породы, так упруго – податливые или жесткопластические элементы, используемые в инженерной практике в качестве защитного экрана для снижения уровня динамических нагрузок на различные подземные сооружения. В данной задаче основание пластического слоя является не жестким, а деформируемым. На основании серии расчетов показана целесообразность и эффективность использования вышеуказанных защитных экранов.

Грунт моделируется неупругой идеальной средой с линейной сжимаемостью и линейной необратимой разгрузкой. Следовательно, сопротивлением среды к сдвиговым усилиям пренебрегается. Согласно данной постановке исследовано влияние деформируемости основания и профиля нагрузки на распределение динамических параметров слоя и контактной поверхности. Сравниваются результаты числового расчета с результатами акустического слоя и слоя жестким основанием. Решение задачи построено в рядах, доказана их сходимость. Рассмотрена задача, когда по верхней границе слоя с основанием движется монотонно убывающая нормальная нагрузка со скоростью *D*, превосходящая скорость распространения волн не меняется, а материал слоя обладает таким свойством, что нагружении и разгрузке связь между давлением P и объемной деформацией ε линейна и необратима, угол наклона E_2 ветви разгрузки диаграммы $P \sim \varepsilon$ превышает угол наклона E_1 ветви нагружении, т.е. $E_1 < E_2$

Также решена задача воздействии подвижной нагрузки на мягкий слой грунта лежащего на полупространстве из более податливого пластического материала. Грунт и материал полупространства моделируется идеальными неупругими средствами. При этом грунт в процессе нагружения имеет ударную диаграмму $P \sim \varepsilon$, а диформирование полупространства подчиняется схеме Прандтля и плотность его материала $\rho_2 < \rho_1$ – плотность грунта. Эта задача обобщает задачу с учетом ударно-волновой процессов в пластической прокладке при воздействии подвижной нагрузки на границу двухслойной среды.

По результатам исследования распространения двумерных волн в многослойном, в частности неоднородном, полупространстве с учетом необратимых процессов в рамках идеальной нелинейно-сжимаемой и линейно-упругой среды можно сделать следующие выводы:

Исследована задача о распространении двумерной пластической волны в двухслойной среде с плотностями ρ_1, ρ_2 для случая когда, диаграмма состояния $P = P(\varepsilon)$ первой среды (грунта) является ударной и при нагружении имеет вид $P(\varepsilon) = \alpha_1 \varepsilon + \alpha_2 \varepsilon^2$, а второй среды (черной породы скалы или прокладки) - упругой или жесткопластической. Задача решается аналитически как прямым, так и обратным методом с учетом волновых процессов

во второй среде и без их учета. Анализ результатов показывает, что при $\rho_1 > \rho_2$ учет упруго – пластических свойств второй среды (прокладки), моделируемой полупространством, приводит, в основном, к уменьшению максимальных значений напряжений (давления) на контакте двух сред. При $\rho_1 < \rho_2$ на контактной поверхности появляется концентрация напряжений и давление получает наибольшее значение в случае акустического слоя, лежащего на жестком основании. Качественная и количественная картина изменения величин давления и кинематических параметров зависит не только от жесткостных характеристик сред, но и от отношения их плотностей.

Таким образом, выше проведенные исследования по изучению двумерного напряженно-деформированного состояния однородной, неоднородной и слоистой среды при интенсивном воздействии подвижной нагрузки на границу многослойного полупространства подтверждают необходимость и важность учета нелинейных, необратимых процессов в среде.

Благодарности

Работа выполнена по программы Грантового финансирования КН МОН РК, РГП на ПХВ Институт информационных и вычислительных технологий КН МОН РК, НИР ИРН AP09562377 по теме: «Разработка математических моделей распространения волн в деформируемых средах при динамических переменных нагрузках с учетом волны разгрузки».

Литература

[1] Рахматулин Х.А., Демьянов Ю.А. Прочность при интенсивных кратковременных нагрузках, Москва, Логос. 2009. 512.

[2] Айдосов А., Айдосов Г.А., Темирбеков Е.С., Тойбаев С. Н., Математическое моделирование распространения ударной нагрузки в сплошных деформируемых средах и взаимодействия двух деформируемых сред при динамических подвижных нагрузках. 2015. 208. ISBN 928-601-263-327-6.

[3] Айдосов А., Темирбеков Е.С., Теория удара. Учебное пособие, Алматы: АТУ, 2015. 64. ISBN 978-601-263-323-8.

[4] Айдосов А., Айдосов Г.А., Калимолдаев М.Н., Тойбаев С. Н., Математическое моделирование взаимодействия балки (пластин, плит, полос) с деформируемым основанием при динамических нагрузках, Монография. - Алматы, 2015. 208.

[5] Айдосов А.А., Айдосов Г.А., Тойбаев С.Н., Дюзбенбетов Б. Распространение двухмерной пластической волны в полуплоскости и отражение. «Актуальные проблемы механики и машиностроение»: материалы международные конференции, Алматы, 2005. 1. 55–59.

[6] Айдосов Г.А., Айдосов А.А., Тойбаев С.Н., Решение задачи о воздействии подвижной нагрузки на неоднородную полуплоскость. Труды международной конференции по распространению упругих и упругопластических волн, посвященной 100-летию со дня рождения Х.А. Рахматулина. Бишкек, 2009. 242-245.

[7] Айдосов А.А., Айдосов Г.А. Тойбаев С.Н., Основные выводы моделирования распространения взрывных волн в многослойном неоднородном полупространстве. *Новости науки Казахстана Научно-технический сборник*. 2009. 2 (101). 56- 60.

[8] Aidosov A., Mamadaliev, N., Khakimov, U. Effect of a mobile load on a nonlinearly compressed strip with a rigid foundation (Article). *Journal of Applied Mechanics and Technical Physics*. 1986. 27(3). 441-445.

[9] Айдосов А.А. Айдосов Г.А., Тойбаев С.Н., Акимханова А. Напряженно-деформационное состояние трубопровода с деформируемом основании при воздействии подвижной напорной нагрузки Вестник КазАТК. Алматы, 2009. 3(58). 133–140.

[10] Айдосов А.А., Айдосов Г.А., Тойбаев С.Н. Основные выводы моделирования распространения взрывных волн в многослойном неоднородном полупространстве. Новости науки Казахстана, Научно-технический сборник. 2009, Выпуск 2 (101), 56- 60.

[11] Li H., Dong Z., Ouyang Z., Liu B., Yuan W., Yin H. Experimental investigation on the deformability, ultrasonic wave propagation, and acoustic emission of rock salt under triaxial compression.

Applied Sciences. 2019. 9(4). 635.

[12] Ишматов М.Р., Авезов А.Х., Рузиев Т.Р., Болтаев З.И., Кульмуратов Н.Р. Распространение естественных волн на многослойном вязкоупругом цилиндрическом теле, содержащем поверхность ослабленного механического контакта. *Journal of Physics: Conference Series*. 2021. 1921(1). 012127. IOP Publishing.

[13] Петров И.Б., Муратов М.В., Сергеев Ф.И. Моделирование распространения упругих волн при разведочном бурении на острове искусственного льда. Прикладная математика и вычислительная механика для интеллектуальных приложений: Труды AMMAI. 2020. 217. 171.

[14] Kumar R., Vohra R., Gorla M. G. Variational principle and plane wave propagation in thermoelastic medium with double porosity under Lord-Shulman theory. *Journal of Solid Mechanics.* 2017. 9(2). 423-433.

[15] Ebrahimi F., Seyfi A., Dabbagh A. The effects of thermal loadings on wave propagation analysis of multi-scale hybrid composite beams. *Waves in Random and Complex Media*. 2021. 1-24.

[16] Stubblefield A. G., Spiegelman M., Creyts T. T. Solitary waves in power-law deformable conduits with laminar or turbulent fluid flow. *Journal of Fluid Mechanics*, 2020, 886.

[17] Ebrahimi F., Dabbagh A. Wave propagation analysis of smart nanostructures.CRC Press, 2019.

[18] Liu T., Li X., Zheng Y., Luo Y., Guo Y., Cheng G., Zhang Z. Study on S-wave propagation through parallel rock joints under in situ stress. *Waves in Random and Complex Media*, 2020, 1-24.

[19] Ebrahimi F., Dabbagh A. Magnetic field effects on thermally affected propagation of acoustical waves in rotary double-nanobeam systems. *Waves in Random and Complex Media.* 2021. 31(1). 25-45.

[20] Kumar R., Sharma N., Lata P., Abo-Dahab S. M. Mathematical modelling of Stoneley wave in a transversely isotropic thermoelastic media. *Applications and Applied Mathematics.* 2017. 12(1).

[21] Li J., Slesarenko V., Galich P. I., Rudykh S. Oblique shear wave propagation in finitely deformed layered composites. *Mechanics Research Communications.* 2018. 87. 21-28.

[22] Ebrahimian H., Kohler M., Massari A., Asimaki D. Parametric estimation of dispersive viscoelastic layered media with application to structural health monitoring. *Soil Dynamics and Earthquake Engineering.* 2018. 105. 204-223.

[23] Cheshmehkani S., Eskandari-Ghadi M. Passive control of 3D wave propagation with a functionally graded layer. *International Journal of Mechanical Sciences.* 2017. 123. 271-286.

[24] Козачка Э., Греловска Г. Теоретическая модель распространения акустической волны на мелководье. *Польские морские исследования*, 2017.

[25] Feng X., Zhang Q., Wang E., Ali M., Dong Z., Zhang G. 3D modeling of the influence of a splay fault on controlling the propagation of nonlinear stress waves induced by blast loading. *Soil Dynamics and Earthquake Engineering*. 2020. 138. 106335.

[26] Singh A. K., Rajput P., Chaki M. S. Analytical study of love wave propagation in functionally graded piezo-poroelastic media with electroded boundary and abruptly thickened imperfect interface. *Waves in Random and Complex Media*. 2020. 1-25.

[27] Li J., Slesarenko V., Rudykh S. Microscopic instabilities and elastic wave propagation in finitely deformed laminates with compressible hyperelastic phases. *European Journal of Mechanics-A/Solids.* 2019. 73. 126-136.

[28] Ai Z. Y., Ye Z. K., Yang J. J. Thermo-mechanical behaviour of multi-layered media based on the Lord-Shulman model.Computers and Geotechnics. 2021. 129. 103897.

[29] Stephan C. C., Schmidt H., Zülicke C., Matthias V. Oblique gravity wave propagation during sudden stratospheric warmings. *Journal of Geophysical Research: Atmospheres.* 2020. 125(1). e2019JD031528.

[30] Kumari N., Chattopadhyay A., Kumar S., Singh A. K. Propagation of SH-waves in two anisotropic layers bonded to an isotropic half-space under gravity. *Waves in Random and Complex Media*. 2017. 27(2). 195-212.

НЕГІЗІ БАР ТОПЫРАҚ ҚАБАТЫНА ЖЫЛЖЫМАЛЫ ЖҮКТЕМЕ ӘСЕРІНЕН ТОЛҚЫНДАРДЫҢ ТАРАЛУЫ

Айдосов Аллаярбек[1], Айдосов Ғалым Аллаярбекович[2],
Нарбаева Салтанат Муратбековна[3]
[1]ҚР БҒМ ҒК "Ақпараттық және есептеу технологиялары институты" ШЖҚ РМК,Алматы қаласы, Қазақстан, allayarbek@mail.ru
[2]ҚазМұнайГаз Аймақ, Нұр-сұлтан қаласы, Қазақстан, galym.aidossov@gmail.com

Распространение волн под воздействием подвижной нагрузки на слое грунта с основанием
Айдосов Аллаярбек, Айдосов Галым Аллаярбекович,
Нарбаева Салтанат Муратбековна

[3]*әл-Фараби атындағы Қазақ ұлттық университеті, Алматы қаласы, Қазақстан,*
narbaevasalta777@gmail.com
[1]ORCID ID: https://orcid.org/0000-0003-2498-4035
[2]ORCID ID: https://orcid.org/0000-0001-6049-4346
[3]ORCID ID: https://orcid.org/0000-0001-5230-3781

Аңдатпа. Математикалық модельдерді әзірлеу мәселесі жұмсақ топырақ қабатындағы жылжымалы жүктеменің әсерінен негізі бар толқындардың таралуы қарастырылады.

Топырақ идеалды сызықты емес сығылатын және қайтымсыз түсіру ортасымен модельденеді, онда жүктеме кезінде және түсіру процесінде қысым мен көлемдік деформация арасындағы байланыс сызықтық және қайтымсыз болады.

Жүктеме қабаттың жоғарғы бетіне қолданылады және сейсмикалық жылдамдықпен қозғалады. Жылжымалы жүктеменің жұмсақ топырақ қабаты мен әртүрлі қалыңдықтағы және тығыздықтағы серпімді төсемнен тұратын екі қабатты ортаға әсері қарастырылады. Мәселені шешу кері және тікелей тәсілдермен аналитикалық түрде жасалады. Бұл тапсырмада медианалық жазықтық жоқ. Сондықтан белгілі бір жағдайларда қабаттың ортаңғы жазықтығына өтетін жазықтық нүктелерінің ығысуы және деформациясы қажетті шамалар ретінде қарастырылады. Деформацияланатын ортадағы толқындық процестерді зерттеуде немесе деформацияланатын негізмен қабаттың өзара әрекеттесу есептерін шешуде математикалық физика әдістері қолданылады.

Түйін сөздер: математикалық модельдер, таралу, пластикалық толқын, аналитикалық шешім, толқынның таралуы, идеалды сұйықтық, сызықтық сығылу, қайтымсыз кему. қозғалыс теңдеуі, үздіксіздік, ортаның жағдайы.

PROPAGATION OF WAVES UNDER THE INFLUENCE OF A MOVING LOAD ON A LAYER OF SOIL WITH A BASE

A. Aydosov[1], G. Aydosov[2], S. Narbayeva[3]

[1]*RSE REM "Institute of Information and Computational Technologies"CS MES RK. Almaty,* allayarbek@mail.ru
[2]*KazMunayGas Aimak, Nur-Sultan,* galym.aidossov@gmail.com
[3]*Al-Farabi Kazakh National University,* narbaevasalta777@gmail.com
[1]ORCID ID: https://orcid.org/0000-0003-2498-4035
[2]ORCID ID: https://orcid.org/0000-0001-6049-4346
[3]ORCID ID: https://orcid.org/0000-0001-5230-3781

Abstract. The problem of developing mathematical models of wave propagation with a base under the influence of a moving load in a layer of soft soil is considered.

The soil is modeled by an ideal nonlinearly compressible and irreversible unloading medium, in which the relationship between pressure and volumetric deformation during loading and during unloading of the medium is linear and irreversible.

The load is applied to the upper surface of the layer and moves at a super seismic speed. The problem of the effect of a moving load on a two-layer medium consisting of a soft layer of soil and an elastic-yielding gasket with different thicknesses and densities is considered. The solution of the problem is constructed analytically in both inverse and direct ways. There is no median plane in the present problem. Therefore, the displacement and deformation of the points of the plane, which under certain conditions passes into the median plane of the layer, are considered as the desired values. Methods of mathematical physics are used in the study of wave processes in deformable media or in solving problems of interaction of a layer with a deformable base.

Keywords: mathematical models, propagation, plastic wave, analytical solution, wave front, ideal fluid, linear compressibility, irreversible unloading. equation of motion, continuity, state of the medium.

Responsible for the release: PhD, Shayakhmetova A.S.

Merkebaev A.

Deputy chief editor: PhD, Mamyrbayev O.Zh

Signed in print 03.03.2020
Edition of 50 copies. Format 60x84 1/16. Paper type.
Order No. 4.

Publication of the Institute of Information and Computational Technologies

28 Shevchenko str., Almaty, Republic of Kazakhstan
7 (727) 272-37-11
atcs@iict.kz