Text Data-Hiding

Nenad O. Vesić[1] and Dušan J. Simjanović[2]

Abstract – **In this paper an algorithm for text data-hiding will be presented. This algorithm protects a personal data. Programs in the software package MATHEMATICA 7.0 will be given. This algorithm is an application of geometry in cryptography.**

Keywords – **curve, matrix, code, key**

I. INTRODUCTION

Group based cryptography was presented in the [1]. Those algorithms are based on the unknown groups. An algorithm which will be presented in this paper is based on the known group (group of regular matrices). In the [2] is presented text data-hiding with set of matrices, where symbols are encoded with one row of a matrix from this set. RSA algorithm [3] is algorithm which is based on large prime numbers. Preferment of the RSA algorithm [3] in this paper will be presented. An algorithm which will be presented in this paper is a combination of algorithms from [1-3]. Large prime numbers are needed in the RSA algorithm. Prime numbers are not required in the algorithm presented in this paper.

II. PRELIMINARY DEFINITIONS

The next tabular is needed for the encrypting using the algorithm which will be presented in this paper.

TABLE 1: THE CHARACTERS

r\c	1	2	3	4	5	6	7
1	0	@	#	{	}	[	%
2	1	.	"	_	:	]	?
3	A	B	C	2	-	=	!
4	D	E	F	3	\	;	/
5	G	H	I	4	×	&	≠
6	J	K	L	5	*	,	~
7	M	N	O	6	^	(	≈
8	P	Q	R	S	7	)	≅
9	T	U	V	8	+	‘	≡
10	W	X	Y	Z	9	°	␣

[1]Nenad O. Vesić is with the Faculty of Science and Mathematics, Višegradska 33, 18000 Niš, Serbia, E-mail: vesic.specijalac@gmail.com
Project: 174012, Serbian Ministry of Science
[2]Dušan J. Simjanović is with the Gimnazija „Svetozar Marković“, Branka Radičevića 1, 18000 Niš, Serbia, E-mail: dsimce@gmail.com

For the matrices $A=[a^i_j]$ and $B=[b^i_j]$ by the type $m\times n$ with integer entries, matrix

$$C=[c^i_j]=[a^i_j b^i_j] \tag{1}$$

is $*-$ ***product*** of the matrices A and B.

Let us define the following operation with matrices:

For a matrix $A=[a^i_j]$ by the type $m\times n$ with non-zero elements, the matrix:

$$\bar{A}=\left[\frac{1}{a^i_j}\right] \tag{2}$$

is $*-$ ***inverse matrix*** of the matrix A.

It is evident that following holds:

$$A*\bar{A}=\begin{bmatrix}1 & \cdots & 1\\ \vdots & \ddots & \vdots\\ 1 & \cdots & 1\end{bmatrix}.$$

The matrices whose entries are the functions of one variable (matrix curves) will be considered in this paper. Let us tell something about those matrices.

Consider the matrix:

$$\boldsymbol{M}=\boldsymbol{M}(t)=[m^i_j(t)] \tag{3}$$

by the type $p\times q$, where:

$$m^i_j:(a,b)\to\mathbf{R}$$

are continuous functions at the interval $(a,b)\subseteq\mathbf{R}$. This matrix is called the ***matrix curve*** at the interval (a,b) by the type $p\times q$.

Elements of the matrix curve could be differential functions of the order $\alpha\in\mathbf{N}$. Thoses matrix curves are α **- differential matrix curves**.

For the α - differential matrix curve $\boldsymbol{M}=\boldsymbol{M}(t)=[m^i_j(t)]$ of the type $p\times q$, the matrix curve:

$$\boldsymbol{M}'(t)=[(m^i_j)'(t)] \tag{4}$$

of the type $p\times q$ is **tangent curve** of the matrix curve M.

Matrix curve:

$$\boldsymbol{M}^{I_0}(t)=[m^{I_0}_j(t)] \tag{5}$$

of the type $1\times n$ is I_0 - **curve** of the matrix curve M for $1\le I_0\le m$.

Algorithms based on tangent vectors of the matrix curves in this paper will be presented.

III. ALGORITHM

Matrix curves with the polynomials of the degree two in this paper will be used. The tabular of the symbols (Table 1.) will be used in this article. This tabular could be arbitrary given.

Matrix curves by the type 5×3 whose entries are polynomials of the degree two encrypt a text-data in the way presented below.

1. Step

Each character is encrypted by a triplet whose coordinates are polynomials of the degree two. Only one of the polynomials has complex roots:

$$z_{1,2}=p\pm iq,$$

where p is an integer between 1 and 10. The parameter $i=p$ (real part of the root z_i) presents the row of the Table 1 where that symbol is. The parameter $j=q\ mod\ r$ where r is the number of element in the $i-th$ row of the Table 1) presents the column of the Table 1 in which that symbol is.

The text is encrypted character-by-character using the ordered set of matrices by the type 5×3. In the matrix, the row which satisfies the previous condition (only one polynomial has complex roots $z_{1,2}=p\pm iq$, $p,q\in\mathbf{Z}, p=\overline{1,10}$) generates the character. If a row does not satisfy previous condition, it generates *access character*. Any text which has $5k$ characters ($k\in\mathbf{N}$) or otherwise, will be supplemented to $5l$ characters ($l\in\mathbf{N}$) with access characters. This supplement is required for avoiding a possible brute force attack in text with standard beginning (diplomatic texts, for example).

2. Step

Let we have the ordered set $\boldsymbol{M}=\{\boldsymbol{M}_1,\cdots,\boldsymbol{M}_l\}$ of the matrix curves which encrypt text-data. System $\boldsymbol{K}=\{\boldsymbol{K}_1,\boldsymbol{K}_2,\cdots,\boldsymbol{K}_l\}=\{[(\boldsymbol{k}_j^i)_s]\}=[m_j^i(0)_s]$, $s=\overline{1,l}$, is important element for hiding.

- Let the ordered sets of matrices $P=\{P_1,P_2,\cdots,P_l\}$ and $Q=\{Q_1,Q_2,\cdots,Q_l\}$ be known like the set of matrix curves
$$\boldsymbol{B}(t)=\{\boldsymbol{B}_1,\cdots,\boldsymbol{B}_l\}=\{\boldsymbol{B}_S\},$$
$$\boldsymbol{B}_S(0)=[0]_{5\times 3},$$
which entries are the polynomials of the degree two.
- Encrypted text-data is:
$$\boldsymbol{C}=\{\boldsymbol{C}_1,\boldsymbol{C}_2,\cdots,\boldsymbol{C}_l\}=$$
$$=\{P_S*(Q_S*\boldsymbol{M}_S+\boldsymbol{B}_S)'\},\qquad(6)$$
$s=\overline{1,l}$.
- The set $\boldsymbol{M}=\{\boldsymbol{M}_1,\cdots,\boldsymbol{M}_l\}=\{\boldsymbol{M}_S\}$ is:
$$\boldsymbol{M}=\{\boldsymbol{M}_1,\boldsymbol{M}_2,\cdots,\boldsymbol{M}_l\}=$$
$$=\{\overline{Q}_S*(\int_0^t(\overline{P}_S*\boldsymbol{C}_S)dt-\boldsymbol{B}_S)+K_S\}\qquad(7)$$
$s=\overline{1,l}$.

Text could be decrypted directly from the descriptions of the matrix curves $\boldsymbol{M}_S$ (step 1). Sets {P, Q, K, B} is private code [4].

The programs are given in the MATHEMATICA 7. 0 in the next section.

IV. PROGRAMS

A. Auxiliary programs

```
PolynomialConstantProduct[a_,p_]:
  =Module[{pcp},c0=a*p/.t->0;c1=a*Dt[p,t]/.t->0;
  c2=a*(Dt[p,{t,2}]/.t->0)/2;pcp=c2*t^2+c1*t+c0;
 pcp];


SystemStarMatrixProduct[a_,b_]:
  =Module[{ssmp=a},For[i=1,i<=Dimensions[a][[1]],i++,
    For[j=1,j<=Dimensions[a[[i]]][[1]],j++,
     For[k=1,k<=Dimensions[a[[i,j]]][[1]],k++,
  ssmp[[i,j,k]]=PolynomialConstantProduct[a[[i,j,k]],b[[i,j,k]]]]]];
 ssmp];
```

Previous two programs are necessary for hiding of a code of the text data.

```
SystemStarInverse[a_]:
  =Module[{ssi=a},For[i=1,i<=Dimensions[a][[1]],i++,
    For[j=1,j<=Dimensions[a[[i]]][[1]],j++,
 For[k=1,k<=Dimensions[a[[i,j]]][[1]],k++,ssi[[i,j,k]]=1/ssi[[i,j,k]]]]];
 ssi];
```

This program returns system b of matrices, generated with the system of matrices which hide text data. Hiding of the hidden text data with system b is encrypted text data.

```
KSetForming[a_]:
  =Module[{ksf=a},For[i=1,i<=Dimensions[a][[1]],i++,
    For[j=1,j<=Dimensions[a[[i]]][[1]],j++,
 For[k=1,k<=Dimensions[a[[i,j]]][[1]],k++,
 ksf[[i,j,k]]=ksf[[i,j,k]]/.t->0]]];
 ksf];
```

The result of this program is system of matrices which presents status of the code which hides a text for $t = 0$.

```
PossibleCodePolynomials[m_]:
  =Module[{pcp={}},For[i=1,i<=Dimensions[m][[1]],i++,
    For[j=1,j<=Dimensions[m[[i]]][[1]],j++,cc=0;nl0=0;
     For[k=1,k<=Dimensions[m[[i,j]]][[1]],k++,
   If[Discriminant[m[[i,j,k]],t]<0,nl0++;cc=k,nl0=nl0]];
   If[nl0==1,pcp=Append[pcp,m[[i,j,cc]]],pcp=pcp]]];
 pcp];
```

The result of this program is set of the polynomials from characters which are not excess characters which hide any chacacter.

```
SymbolPositions[m_,key_]:
  =Module[{sp={}},pcp=PossibleCodePolynomials[m];
    For[i=1,i<=Dimensions[pcp][[1]],i++,
     rr=-(Dt[pcp[[i]],t]/.t->0)/Dt[pcp[[i]],{t,2}];
     cc=Abs[Discriminant[pcp[[i]],t]/Dt[pcp[[i]],{t,2}]];
    If[(IntegerQ[rr])&&(1<=rr<=10)&&(IntegerQ[cc]),
    If[Mod[cc,Dimensions[key[[rr]]][[1]]]==0,
     cc=Dimensions[key[[rr]]][[1]],
      cc=Mod[cc,Dimensions[key[[rr]]][[1]]]],cc=0];
  If[cc!=0,sp=Append[sp,{rr,cc}],sp=sp]];
 sp];
```

Result of this program is the set of positions of symbols from the encrypted text. Those positions need one step more for finding of final positions. Parameter j must be found.

B. Main programs

```
CodeHiding[p_,q_,b_,m_]:
  =Module[{ch},k=KSetForming[m];hm=m-k;
  fd=SystemStarMatrixProduct[q,hm]+b;
    der=Dt[fd,t];ch=SystemStarMatrixProduct[p,der];
 ch];
```

This program hides encrypted text data.

```
CodeDehiding[p_,q_,b_,k_,c_]:
  =Module[{cd},ip=SystemStarInverse[p];iq=SystemStarInverse[q];
    fs=SystemStarMatrixProduct[ip,c];ss=Integrate[fs,t];ts=ss-b;
 fthss=SystemStarMatrixProduct[iq,ts];cd=fthss+k;
 cd];
```

The result of this program is code which was hidden.

```
DecodingPositions[p_,q_,b_,k_,c_,key_]:
  =SymbolPositions[CodeDehiding[p,q,b,k,c],key];
```

The result of this program is the final set of the positions of symbols in the tabular 1.

C. *Explanations of previous programs*

Auxiliary programs execute the operations defined in the introduction. Program *CodeHiding* hides primary code of the text. Result of the program *DecodingPositions* is set of positions of characters in the encrypted text.

V. CONCLUSION

In this paper text data-hiding algorithm was presented. The texts could be encrypted with large numbers (not necessary primes like in the RSA algorithm), like coefficients of the polynomials. There exists only one problem using encrypting/decrypting algorithm presented in this paper. The problem is to create a code.

Factorization attack is impossible because of the set of matrix curves B, while brute force attack is impossible because of the large coefficients of the polynomials which encrypts the text.

REFERENCES

[1] Alexei Myasnikov, Vladimir Shpilrain, Alexander Ushakov, *Group-based cryptography*, Birkhauser, 2008.

[2] R. Villan, S. Voloshynovskiy, O. Koval, J. Vila, E. Topak, F. Deguillaume, Y. Rystar, T. Pun, *Text Data-Hiding for Digital and Printed Documents*: *Theoretical and Practical Considerations*, http://cvml.unige.ch/publications/postscript/2006/SPIE-EI-2006-Text-Data-Hiding-paper.pdf

[3] RSA. Wikipedia [Online], http://en.wikipedia.org/wiki/RSA

[4] Private-key (or secret-key) cryptography. *Kioskea.net* [Online] http://en.kioskea.net/contents/crypto/cleprivee.php3