Encryption System based on a Structured Matrix: *Vandermonde Matrix*

Hana Ali-Pacha, Naima Hadj-Said and Adda Ali-Pacha

LACOSI: Lab. de Coding and Security of Information

University of Sciences and Technology of Oran,
Po Box 1505 Oran M'Naouer Algeria
hana.alipacha@univ-usto.dz; nim_hadj@yahoo.fr; a.alipacha@gmail.com

Keywords: Cryptography, Matrix Structured, Vandermonde, Symmetrical key

Abstract: The development of communications and digital transmissions have pushed data encryption to grow quickly to protect the information against any hacking or digital plagiarisms. Also, the matrix computation algorithms developed since the fifties exploit different types of structures more algebraically. In this work, we will propose an encryption system based on the Vandermonde matrix, to secure the data in the form of images. Some orders will be advanced MatLab programming.

1 INTRODUCTION

With the advent of the Internet and, the computer communication networks (LANs, metropolitan and wide area networks) and the use of satellite links, the new industrial revolution in computing and telecommunications has resulted [1, 2, 3] in the storage and transmission of large amounts of confidential data and a growing concern to protect their access. Encryption is required for their data not intelligible except for the audience wanted.

The search for other encryption systems is still valid. The objective in this work is to make available to the encryption, a cryptosystem based on structured matrix specially the Vandermonde matrix.

2 STRUCTURED MATRICES

Many problems in applied mathematics [4, 5] require solving linear systems of size n × n. For small systems, there is no great advantage to using non-standard resolution algorithms. However, n can be very large, and sometimes these systems must be solved multiple times. In such cases, the standard algorithms based on Gaussian elimination require $O(n^3)$ arithmetic operations for a system of size n × n, and it will be a handicap for the calculation.

That is why we are trying to use the structure of matrix, to reduce the computation time. Structures of sparse matrices, bands, triangular, symmetric ... but also Toeplitz, Hankel, Vandermonde, Cauchy and many other types which are commonly used. The computational complexity with a structured matrix of size n × n is much lower than for a general matrix of size n × n. The best known are the Toeplitz matrices and Hankel, but the Vandermonde matrix is also familiar. These are useful for their applications in celestial mechanics and the algebraically decoding.

In the case of cryptography, we can define three classes of matrix which can be used:

- Type Toeplitz,
- Type Hankel,
- Type Vandermonde.

Let us quickly recall the definition of these algebraic structures: a Toeplitz matrix (resp. Hankel) is constant along its downward diagonal (resp. riser), the general term of a Vandermonde matrix is of the form $(x_i)^j$.

Toeplitz matrix: A is a Toeplitz matrix [5] when all diagonal elements are similar as follows:

$$\boldsymbol{A} = \begin{bmatrix} a_1 & a_{-2} & a_{-3} & \cdots & a_{-n} \\ a_2 & a_1 & a_{-2} & \cdots & \vdots \\ a_3 & a_2 & a_1 & \ddots & a_{-3} \\ \vdots & \ddots & \ddots & \ddots & a_{-2} \\ a_n & \cdots & a_3 & a_2 & a_1 \end{bmatrix}$$

Henkel matrix: H is a matrix of Henkel [5] when all the elements of s anti-diagonals are similar as follows:

$$\boldsymbol{H} = \begin{bmatrix} z_{N-1} & z_{N-2} & z_{N-3} & \cdots & z_0 \\ z_{N-2} & z_{N-3} & z_{N-4} & . \cdot & z_{-1} \\ z_{N-3} & z_{N-4} & z_{N-5} & . \cdot & z_{-2} \\ \vdots & \iddots & \iddots & \iddots & \vdots \\ z_0 & z_{-1} & z_{-2} & \cdots & z_{-(N-1)} \end{bmatrix}$$

Vandermonde matrix: The Vandermonde matrix [5] of the following form:

$$\boldsymbol{V} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ a_1^2 & a_2^2 & \cdots & a_n^2 \\ \vdots & \vdots & & \vdots \\ a_1^{m-1} & a_2^{m-1} & \cdots & a_n^{m-1} \end{bmatrix}$$

Circulating matrix: A matrix C(r) square of size n×n is called circulating matrix [6], if it has the following form:

$$C(r) = \begin{pmatrix} r_0 & r_{n-1} & \cdots & r_1 \\ r_1 & r_0 & \cdots & r_2 \\ \vdots & \ddots & \ddots & \vdots \\ r_{n-1} & \cdots & r_1 & r_0 \end{pmatrix}.$$

2.1 Vandermonde matrix

In linear algebra, a Vandermonde matrix is a matrix with a geometric progression in each row. It takes its name from Alexandre-Théophile Vandermonde. This matrix looks like this:

$$V = \begin{pmatrix} 1 & \alpha_1 & {\alpha_1}^2 & \dots & {\alpha_1}^{n-1} \\ 1 & \alpha_2 & {\alpha_2}^2 & \dots & {\alpha_2}^{n-1} \\ 1 & \alpha_3 & {\alpha_3}^2 & \dots & {\alpha_3}^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_m & {\alpha_m}^2 & \dots & {\alpha_m}^{n-1} \end{pmatrix}$$

In other words:

$$\forall\ i \text{ et } j,\ V_{i,j} = (\alpha_i)^{j-1}$$

Some authors use the transpose of this matrix.

Consider a square matrix Vandermonde V (m = n). It is invertible if and only if the α_i are pairwise distinct. If two coefficients α_i are identical, the matrix has two identical rows, so is not invertible.

2.2 Relationship between Structured Matrices

A relationship between two types of structured matrices meant a rapid transformation of the first type to the second type, by multiplication of matrices that we know to reverse quickly and multiply rapidly by a vector.

For a relationship between Toeplitz and Hankel kind. It suffices to multiply a Toeplitz matrix by the J matrix to have a Hankel matrix, and vice versa.

The matrix J_n, of size n × n, will be J if there is no confusion. The J matrix is symmetric and orthogonal, Thus, J^2= I.

$$J_3 = J = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

One seeks to find relationships between other types.

3 ENCRYPTION PRINCIPLE

1. To encrypt our pictures we will generate a Vandermonde matrix, using a character string, pairwise distinct, which will be converted to ASCII binary values. The chain length is 4.

Example: the character string "USTO" is converted to α_i = [85 83 84 79].

2. Then we divide the number sequence by 256, to get all the number sequence lower of one.

Dividing in the previous example we obtain 256 [0.3320 0.3242 0.3281 0.3086].

3. One constructed the Vandermonde matrix V as :

$$V = \begin{bmatrix} 0.0366 & 0.1102 & 0.3320 & 1.0000 \\ 0.0341 & 0.1051 & 0.3242 & 1.0000 \\ 0.0353 & 0.1077 & 0.3281 & 1.0000 \\ 0.0294 & 0.0952 & 0.3086 & 1.0000 \end{bmatrix}$$

4. We will arrange the columns of the matrix V so to have in all the diagonal 1, the ciphering matrix M_c is obtained as :

This is obtained with the displacement of the positions of columns for each line:

$$M_c = \begin{bmatrix} 1.0000 & 0.0366 & 0.1102 & 0.3320 \\ 0.3242 & 1.0000 & 0.0341 & 0.11051 \\ 0.1077 & 0.3281 & 1.0000 & 0.0353 \\ 0.0294 & 0.0952 & 0.3086 & 1.0000 \end{bmatrix}$$

5. We will use the encryption function as follows as :

$$y = M_c * x$$

The coordinates of the vector y are decimal. The plaintext vector x contains 4 pixels of data, which is divided by the 256.

- $y_1 = x_1 + (\alpha_1).x_2 + (\alpha_1)^2.x_3 + (\alpha_1)^3.x_4$
- $y_2 = (\alpha_2)^3.x_1 + x_2 + (\alpha_2).x_3 + (\alpha_2)^2.x_4$
- $y_3 = (\alpha_3)^2.x_1 + (\alpha_3)^3.x_2 + x_3 + (\alpha_3).x_4$
- $y_4 = (\alpha_4).x_1 + (\alpha_4)^2.x_2 + (\alpha_4)^3.x_3 + x_4$

It is convenient to introduce the notation of:

$$M_c = L+D+U$$

Where L is a strictly lower triangular matrix. D is a diagonal matrix (D = I), U is an upper triangular matrix strictly.

$$y = M_c * x = (L + D + U) * x$$

$$y = x + (\mathrm{L} + \mathrm{U}) * \mathrm{x}$$

6. Y are multiplied by a value M≥1000, then by taking the modulo 256 of the integer part :

$$yd = mod(floor(y * M), 256)$$

The yd is the ciphertext vector of x plaintext vector.

3.1 Encryption key

Encryption requires a 56-bit key length, with the following fields:

1. One word of 4 characters (ASCII) pairwise distinct: 4x8 = 32 bits.
2. The order of the characters of the words, i.e. swap function: 2x4 = 8 bits.
3. The value M: 16 bits

3.2 Decryption Method

We proposed toadopt the Jacobi method [7, 8], for decoding system. This is an itertive method for solving a matrix system of the form Ax = b. For this, a sequence $x^{(k)}$ which converges to a fixed point x, solution of the system of linear equations.

We look to build for a given value $x^{(0)}$ the sequence follows:

$$x^{(k+1)} = F(x^{(k)}) \quad \text{with } k \in N$$

$$Ax=b \Leftrightarrow (L + D + U)x=y \Leftrightarrow$$
$$D^{(-1)}Dx = D^{(-1)}(y - (L+U))x =$$

D is diagonal matrix, thus invertible .

$$x = - D^{(-1)}((L+U))x + D^{(-1)}y = F(x)$$

Where F is an affine function. $D^{(-1)}(L+U)$ is then called **Jacobi Matrix**.

Since D is unitary, the generic iteration for our method is then:

$$x^{(k+1)} = -(L+U)x^{(k)} + y$$

A sufficient but not necessary to guarantee convergence of the condition of the Jacobi iteration is the diagonal dominance.

A matrix A∈ $R^{n\times n}$ is said to be strictly diagonally dominant if:

$$|a_{ii}| > \sum_{\substack{j=1,\\ j\neq i}}^{n} |a_{ij}| \qquad i = 1, \dots, n.$$

In this case, it is checked easily:

$$\|D^{-1}(L+U)\|_\infty = \max_{1\leq i\leq n} \sum_{\substack{j=1\\ j\neq i}}^{n} \left|\frac{a_{ij}}{a_{ii}}\right| \leq 1$$

The matrix M_c is a matrix diagonally dominant. For the convergence of the method the following theorem is applied:

Let $e^{(k)}$ the error vector:

$$e^{(k+1)} = x^{(k+2)} - x^{(k+1)} = D^{(-1)}(L+U)(x^{(k+2)} - x^{(k+1)})$$
$$= D^{(-1)}(L+U)\, e^{(k)}$$

We set B= $D^{(-1)}(L+U)$, which gives

$$e^{(k+1)} = B\, e^{(k)} = B^{(k+1)}\, e^{(0)}$$

The algorithm converges if:

$$lim_{k\to\infty}\|e^{(k)}\| = 0 \Leftrightarrow lim_{k\to\infty}\|B^{(k)}\| = 0$$

(i.e. B^k tends towards zero matrix).

Theorem 1: A necessary and sufficient condition for that

$$lim_{k\to\infty}\|B^{(k)}\| = 0$$

Is that the spectral radius (the largest eigenvalue in modulus) of **'B is strictly less than 1.**

Theorem 2: The method converges for any value $x^{(0)}$ for linear systems whose matrix is strictly diagonally dominant.

We have taken $x^{(0)} = y$ (Theorem 2).

$$y = M_c * x = (L + D + U) * x$$

$$x = y - (\mathrm{L} + \mathrm{U}) * \mathrm{x}$$

$$x = y - (\mathrm{L} + \mathrm{U}) * (y - (\mathrm{L} + \mathrm{U}) * \mathrm{x})$$

$$x = y - (L + U) * y + (L + U)^2 * x$$

$$x = y - (L + U) * y + (L + U)^2 * (y - (\mathrm{L} + \mathrm{U}) * \mathrm{x})$$

$$x = y - (L + U) * y + (L + U)^2 * y - (L + U)^3 * \mathrm{x}$$

According to the theorem 1 we have:

$$x = y + \sum_{i=1}^{k} ((-1)^i (L + U)^i * y)$$

$$x = (I + \sum_{i=1}^{k} (-1)^i (L + U)^i) * y$$

We put

$$M_d = (I + \sum_{i=1}^{k} (-1)^i (L + U)^i)$$

The decryption function is then:

$$x = M_d * y$$

For the stopping test, the relative error will be used on the residue vector to an accuracy of $(10)^{-9}$.

The Jacobi method has a cost in the order of $(3n^2+2n)$ per iteration. Nevertheless, it is very easily parallelizable.

5 CONCLUSIONS

The proposed system produces two matrices M_c and M_d respectively for encryption and decryption.

We have found that the security of this crypto system is acceptable. So, it offers a high level of security and is easily usable.

REFERENCES

[1] B. Schneier," Applied Cryptography-Protocols, Algorithms and Source Code in C", John Wiley & Sounds, Inc, New York, Second Edition, 1996.

[2] Beckett Brian : " Introduction aux méthodes de la cryptologie", Editions Masson, 1990.

[3] Marsault Xavier : " Compression et cryptage des données multimédias", 2e édition revue et augmentée, Editions Hermès, 1992.

[4] Houssam KHALIL, "Matrices structurées et matrices de Toeplitz par blocs de Toeplitz en calcul numérique et formel ", THÈSE DE DOCTORAT, l'UNIVERSITÉ CLAUDE BERNARD - LYON 1, defended on 25th of July 2008.

[5] T. Kailath and A. H. Sayed, editors. Fast reliable algorithms for matrices with structure. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 1999.

[6] Gregory Ammar and Paul Gader. A variant of the Gohberg-Semencul formula involving circulant matrices. SIAM J. Matrix Anal. Appl., 12(3) :534–540, 1991.

[7] G. Allaire, S.M. Kaber, Numerical linear algebra.. Ellipses, 2002

[8] M. Schatzmann, Numerical Analysis, A Mathematical Introduction. Oxford University Press, 2002.

[9] Guanrong Chen, Yaobin Mao, Charles K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps", doi:10.1016/j.chaos.2003.12.022, Chaos, Solitons and Fractals 21, pp: 749–761, 2004.