Алексей Стахов, Мустафа Калами Херис

Матричная криптография для цифровых сигналов

Matrix cryptography for digital signals

Alexey Stakhov
International Club of Golden Section, Canada

S. Mostapha Kalami Heris
Ferdowsi University of Mashhad, Iran

Расширенная аннотация (А.П. Стахов)

Эта статья явилась результатом моего сотрудничества с иранским исследователем **S. Mostapha Kalami Heris,** которого заинтересовали некоторые мои статьи, касающиеся криптографии [4-7]. Суть идей, изложенных в работах [4-7], состояла в том, чтобы использовать специальный класс матриц, называемых матрицами Фибоначчи и «золотыми» матрицами, для кодирования информации, с целью ее защиты от искажений (корректирующие коды) и от несанкционированного доступа (криптография). При этом использовался «матричный метод» кодирования и декодирования. В этом методе исходная информация подставлялась в матричной форме, то есть в виде квадратной матрицы определенного размера. Затем эта матрица умножалась на *кодирующую матрицу* (матрицу Фибоначчи или «золотую» матрицу) того же размера, при этом получалась *кодовая матрица*, элементы которой направлялись в канал связи. Декодирование состояло в умножении кодовой матрицы, полученной из канала связи, на *декодирующую матрицу*, которая была инверсной к *кодирующей матрице*. В книге [4] и статье [5] было показано, что с использованием некоторых уникальных математических свойств матриц Фибоначчи на этой основе могут быть созданы корректирующие коды, которые обладают фантастической корректирующей способностью по сравнению с известными алгебраическими кодами (в 1 000 000 раз лучше, чем классические корректирующие коды). Кроме того, в предлагаемом методе кодирования объектами коррекции являются не биты и их сочетания, а элементы кодовой матрицы, которые могут быть числами огромной величины. Ясно, что **такая теория корректирующих кодов представляет большой интерес для создания супернадежных информационных систем.**

В статьях [6, 7] эта же идея использовалась для криптографической защиты информации. При этом использовались так называемые «золотые» матрицы, элементами которых являются гиперболические функции Фибоначчи, введенные в работе: Stakhov A., Rozin B. *On a new class of hyperbolic function*. Chaos, Solitons & Fractals, 2005, Volume 23, Issue 2, 379-389.

Mostapha Kalami Heris в своем письме ко мне обратил мое внимание на то, что в качестве кодирующей и декодирующей матриц могут использоваться не только матрицы Фибоначчи или «золотые» матрицы, но и более широкий класс матрицы, известных в теории матриц как *неособенные матрицы* (*non-singular matrices*). Главной «особенностью» неособенных матриц является то, что их детерминант отличается от нуля. Меня заинтересовала эта идея, и мы начали исследовать такой метод криптографии. Мне пришлось глубже вникнуть в такую область информатики как *криптография* [1-3]. В результате изучения литературы по этой теме [1-3] удалось установить следующее:

1. Наиболее предпочтительной в современных криптографических системах считается «*криптосистемы с открытым ключом*», называемые также *«асимметричными криптосистемами»*. В «асимметричных криптосистемах» используется два «криптографических ключа»:

- *открытый ключ*, который выставляется для всеобщего обозрения;
- *секретный ключ*, известный только получателю сообщения.

На передающей стороне с помощью «открытого ключа» формируется кодовое сообщение, которое направляется в «канал связи». Без знания «секретного ключа» расшифровать кодовое сообщение невозможно. Однако, получатель, знающий «секретный ключ», расшифровывает закодированное сообщение.

Основным достоинством «асимметричных криптосистем» [1], что стало причиной их широкого распространения в криптографической практике, является тот факт, что нет необходимости пересылать «секретный ключ» от получателя к отправителю сообщения.

2. В то же время «асимметричные криптосистемы» имеют существенный недостаток» по сравнению с «симметричными криптосистемами», на который обращается внимание в работах [2, 3]. Дело в том, что «асимметричные криптосистемы» значительно медленнее по сравнению с «симметричными криптосистемами», что затрудняет использование «асимметричных криптосистем» в информационных системах, работающих в реальном масштабе времени (примером таких информационных систем является *цифровая телефония*). В работе [3] отмечается, что «*существенным недостатком «асимметричных алгоритмов» является то, что они гораздо медленнее (в 1000 и более раз) в сравнении с «симметричными алгоритмами»*.

Криптографическая практика нашла изящный выход для преодоления указанного недостатка «асимметричных криптосистем». Было выдвинута концепция «гибридных криптосистем» [2, 3]. Концепция *гибридной криптосистемы* [2, 3] является новым направлением в криптографии, которая объединяет преимущества «асимметричных криптосистем» с эффективностью «симметричных криптосистем». *Гибридная криптосистема* может быть сконструирована на основе двух раздельных криптосистем:

- «асимметричная криптосистема», которая используется для **передачи криптографических ключей;**
- «симметричная криптосистема», которая используется для **передачи данных.**

Предположим, что Боб и Алиса решили обменяться сообщениями. Предполагается, что у Боба и Алисы имеются «открытые криптографические ключи», используя которые они могут передавать некоторые сообщения в «медленном» режиме.

Предположим, что Боб желает передать Алисе сообщение *m* с использованием «гибридной криптосистемы». Для этого он делает следующее:

- Генерирует случайным образом «симметричный криптографический ключ» (скажем, *s*).
- Шифрует сообщение *m* с использованием «симметричной криптосистемы», используя ключ *s*.
- Шифрует ключ *s* , используя «публичный криптографический ключ» Алисы.
- Отсылает оба шифрованных сообщения Алисе.

Алиса использует свой «секретный криптографический ключ» для дешифрации ключа *s*, и затем использует ключ *s* для дешифрации сообщения *m*.

Ясно, что концепция *гибридной криптосистемы* позволяет объединить все преимущества «асимметричных» и «симметричных» криптосистем. Такой подход повышает интерес к новым криптографическим алгоритмам, в частности, к *матричной криптографии.*

Второй вопрос, который мы решали вместе с Mostapha Kalami Heris, - это поиск области эффективного использования *матричной криптографии.* Мы пришли к выводу, что наиболее эффективной областью является передача *цифровых сигналов,* примером которых является цифровая телефония, аудио и видеосигналы и т.д. В таких системах допускается некоторая погрешность при дешифрации сообщений. В качестве примера можно привести использование аналого-цифровых и цифро-аналоговых преобразователей (АЦП и ЦАП), которые широко используются в цифровой телефонии, аудио и видео системах. Ясно, что погрешность АЦП и ЦАП влияет на качество воспроизведения телефонного сигнала или аудио и видеосигнала. Но при достаточно высокой точности АЦП и ЦАП человеческий слух или зрение не в состоянии отличить отклонение сигнала от истинного сигнала. Подобное же происходит при использовании матричной криптографии. При шифрации и дешифрации могут происходить некоторые отклонения дешифрованного сигнала от исходного, но, благодаря особенностям человеческого восприятия, это не оказывает существенного влияния на качество передачи *цифрового сигнала.*

Итак, главная задача настоящей статьи – дать обоснование нового криптографического метода, названного *матричной криптографией*, который может быть использован в рамках «гибридной криптосистемы» для «быстрой» передачи цифровых сигналов в реальном масштабе времени.

Статья состоит из четырех частей. Во **Введении** дается определение *цифрового сигнала* и рассматриваются примеры квадратных матриц (матриц Фибоначчи и «золотых» матриц), которые были использованы в моих первых работах [4-7] для кодирования и декодирования.

В параграфе 2 «**Non-singular matrices» (Неособенные матрицы)** излагается основы теории неособенных матриц, которые используются для кодирования и декодирования при матричной криптографии. Квадратная матрица A называется неособенной, если ее детерминант отличается о нуля, то есть,

$$\det A \neq 0 .$$

Каждая неособенная матрица имеет *инверсную матрицу* A^{-1}, которая связана с исходной матрицей следующим соотношением:

$$AA^{-1} = I_n ,$$

где I_n - единичная матрица размера n.

Существует следующее свойство неособенных матриц:

$$\det\left(A^p\right) = \left(\det A\right)^p$$

Простейшая неособенная квадратная $(2\times 2)-$матрица имеет вид:

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

Ее детерминант вычисляется по формуле:

$$\det A = a_{11}a_{22} - a_{12}a_{21} \neq 0 .$$

Ее инверсная матрица вычисляется по формуле:

$$A^{-1} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}^{-1} = \frac{1}{\det A}\begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}.$$

Далее излагаются основы теории неособенных $(n\times n)-$матриц $(n>2)$ и способы нахождения инверсных матриц.

В параграфе **Matrix Approach to Cryptography (Матричный подход к криптографии)** излагается общий принцип *матричной криптографии*. Рассмотрим неособенную матрицу E и ее инверсную матрицу E^{-1}. Матрица E являются *кодирующей матрицей* и одновременно *криптографическим ключом*, матрица E^{-1} может быть вычислена известным способом с использованием матрицы E. Пусть X – исходное сообщение, представленное в виде квадратной матрицы того же размера, что и *кодирующая матрица* E. Тогда *шифрация* состоит в перемножении матриц E и X. В результате образуется *зашифрованное сообщение* Y:

$$Y = E \times X$$

Дешифрация состоит в умножении *зашифрованного сообщения* Y на инверсную матрицу E^{-1}:

$$E^{-1}\times Y = E^{-1}\times\left(E\times X\right) = \left(E^{-1}\times E\right)\times X = I\times X = X$$

Далее приводятся примеры шифрации и дешифрации для звукового сигнала и для некоторого видео-образа.

В **Заключении** еще раз анализируются преимущества *матричной криптографии*, основанной на концепции «гибридной криптосистемы». Матричная криптография основана на матричном умножении и обеспечивает быстрое преобразование цифрового сигнала в зашифрованное сообщение, что позволяет использовать ее для криптографической защиты цифровых сигналов, поступающих в реальном масштабе времени. «Криптографический ключ» (кодирующая матрица) может изменяться случайным образом достаточно часто, что обеспечивает хорошую степень криптографической защиты. Ясно, что в данной статье излагается только идея

метода. Для его практического использования необходимо провести дополнительные исследования.

Первым реальным проектом может стать создание чипов на основе предлагаемого метода, которые могут быть встроены в ***мобильный телефон*** для криптографической зашиты телефонных сообщений.

Abstract

In this study we develop a new method of cryptography based on matrix approach. Digital signals (including digital sound signals and digital images), which are used widely in modern media products, are real area of application of the matrix cryptography. This method refers to symmetric-key cryptography. As cryptographic key, the method uses special kernel matrix, which is non-singular matrix, and some real number *p*, which is used as a power of the kernel matrix. In order to transmit cryptographic key from Sender to Receiver, we can use public-key cryptosystem. Matrix cryptography can be used effectively for protection of digital music and digital movies from forbidden access.

1. Introduction

In this study we are talking about cryptographic protection of **digital signals.** The term of **digital signal** used in the present article refers to discrete-time signals that have a discrete number of levels. **Digital signals** are digital representations of discrete-time signals, which are often derived from analog signals. In the Digital Revolution, the usage of digital signals has increased significantly. Many modern media devices, especially the ones that connect with computers use digital signals to represent signals that were traditionally represented as continuous-time signals; measurement systems, cell phones, music and video players, personal video recorders, and digital cameras are examples.

Let us represent a digital signal X in the form of sequence of samples $\{x_i; i = 1,2,3,...\}$, that is,

$$X = \{x_1, x_2, x_3, x_4, x_1, x_2, x_3, x_4, ..., x_{n+1}, x_{n+2}, x_{n+3}, x_{n+4}, ...\} \quad (1)$$

It is clear that for many cases there is a problem of cryptographic protection of digital signal (1). First of all, it is important to protect cell phones from forbidden hearing. Other example is to protect music or video information from forbidden access. Also it is very important to protect many measurement systems from forbidden access and so on. Possibly, such problems exist for video recorders, and digital cameras.

As is well-known, a majority of continuous-time signals are signals representing information in real scale of time. Of course, cryptographic algorithms used for cryptographic protection of digital signals should be enough fast-acting algorithms.

Let us consider from this point of view public-key algorithms [1] used very widely in modern cryptographic praxis. Many famous specialists are evaluating the advantages of public-key cryptography very critically and are paying attention to shortcomings of public-key cryptography. **Richard A. Molin** writes in [2]: “Public-key methods are extremely slow compared with symmetric-key methods. In latter discussions we will see how both the public-key and symmetry-key cryptosystems come to be used, in concert, to provide the best of worlds combining the efficiency of the symmetric-key ciphers with the increased security of public-key ciphers, called hybrid systems.” As is noted in [3], “one drawback of asymmetric key algorithms is that they are much slower (factors of 1000+ are typical) than 'comparably' secure symmetric key algorithms. In many quality cryptosystems, both algorithm types are used. The receiver's public key encrypts a symmetric algorithm key which is used to encrypt the main message. This combines the virtues of both algorithm types when properly done. Such cryptographic systems are called hybrid cryptosystems.”

A concept of *hybrid cryptosystem* is a new direction in cryptography [2, 3], which combines convenience of a public-key cryptosystem with the efficiency of symmetric-key cryptosystems. A hybrid cryptosystem can be constructed using two separate cryptosystems:

- a public-key cryptosystem for the **transmission of cryptographic keys**, and

- a symmetric-key cryptosystem for **data transmission**.

The hybrid cryptosystem is itself a public-key system, who's public and private keys are the same as in the scheme for the transmission of cryptographic keys.

To encrypt a message *m* addressed to Alice in a hybrid scheme, Bob does the following:

- Generates a random (private) key for the data encapsulation scheme (say, *s*).
- Encrypts the message *m* under the data encapsulation scheme, using the key *s* just generated.
- Encrypts the key *s* under the key encapsulation scheme, using Alice's public key.
- Sends both of these encryptions to Alice.

Alice can use her private key to decrypt *s*, and then use *s* to decrypt the message *m*.

It is clear that a concept of "hybrid cryptosystem" allows to unite effectively all advantages of public-key and symmetric-key cryptosystems. Such approach raises interest in the development of hybrid cryptography based on new cryptographic algorithms.

Recently in the works by **Alexey Stakhov** [4-7] a matrix approach to coding theory and cryptography based on the Fibonacci and "golden" matrices was developed.

Let us consider examples of the Fibonacci matrices. For the first time, a concept of the Fibonacci *Q*-matrix

$$Q=\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix} \qquad (2)$$

was developed in **Hoggatt**'s book [8]. It is a generating matrix for the classical Fibonacci numbers F_n

$$F_n= F_{n-1}+ F_{n-2};\quad F_0=0,\ F_1=1. \qquad (3)$$

The *Q*-matrix (2) possesses the following mathematical properties:

$$Q^n=\begin{pmatrix}F_{n+1} & F_n\\ F_n & F_{n-1}\end{pmatrix} \qquad (4)$$

$$\det Q^n=F_{n-1}F_{n+1}-F_n^2=(-1)^n. \qquad (5)$$

Every "direct" matrix (4) has its own inverse matrix that takes two different forms in dependence on parity of *n*. For the even $n=2k$ the inverse matrix Q^{-n} has the following form:

$$Q^{-2k}=\begin{pmatrix}F_{2k-1} & -F_{2k}\\ -F_{2k} & F_{2k+1}\end{pmatrix}; \qquad (6)$$

for the odd $n=2k+1$ the inverse matrix Q^{-n} has the form:

$$Q^{-2k-1}=\begin{pmatrix}-F_{2k-2} & F_{2k+1}\\ F_{2k+1} & -F_{2k}\end{pmatrix}. \qquad (7)$$

Alexey Stakhov developed in [9] a theory of Fibonacci Q_p-matrices, which are a generalization of the *Q*-matrix (2). For a given $p=0, 1, 2, 3, \ldots$ the Q_p-matrix is a $(p+1)\times(p+1)$-matrix of the kind

$$Q_p=\begin{pmatrix}1 & 1 & 0 & 0 & \cdots & 0 & 0\\ 0 & 0 & 1 & 0 & \cdots & 0 & 0\\ 0 & 0 & 0 & 1 & \cdots & 0 & 0\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\ 0 & 0 & 0 & 0 & \cdots & 1 & 0\\ 0 & 0 & 0 & 0 & \cdots & 0 & 1\\ 1 & 0 & 0 & 0 & \cdots & 0 & 0\end{pmatrix}. \qquad (8)$$

The Fibonacci Q_p-matrix (8) is a generating matrix for the Fibonacci *p*-numbers $F_p(n)$ introduced by **Alexey Stakhov** in [10]:

$$F_p(n)= F_p(n)+ F_p(n-p-1);\ F_p(0)=0,\ F_p(1)=F_p(2)=\ldots=F_p(p)=1. \qquad (9)$$

The recurrence relation (9) is reduced to the recurrence relation (3) for the classical Fibonacci numbers ($p=1$). Also the Fibonacci *p*-numbers (9) follow directly from Pascal triangle [10].

If we raise the Q_p-matrix (8) to n-th power, we get [9]:

$$Q_p^n = \begin{pmatrix} F_p(n+1) & F_p(n) & \cdots & F_p(n-p+2) & F_p(n-p+1) \\ F_p(n-p+1) & F_p(n-p) & \cdots & F_p(n-2p+2) & F_p(n-2p+1) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ F_p(n-1) & F_p(n-2) & \cdots & F_p(n-p) & F_p(n-p-1) \\ F_p(n) & F_p(n-1) & \cdots & F_p(n-p+1) & F_p(n-p) \end{pmatrix}. \qquad (10)$$

It is proved in [9] that the determinant of the matrix (9) is equal to

$$\det Q_p^n = (-1)^{np}. \qquad (11)$$

An essence of this approach consists of the following. The initial message X (the data message) is represented in the form of square matrix of the size $p \times p$, where p is some integer, which takes its values from the set $\{2,3,4,...\}$. The matrix X is multiplied by special encoding matrix E of the same size to get the code matrix Y. The matrix E has inverse matrix E^{-1}. A decoding consists in multiplication of the code matrix Y by the inverse decoding matrix E^{-1}. If we use the so-called Fibonacci matrices (4) and (10) and inverse to them matrices of the kind (6) and (7) as encoding and decoding matrices, we can detect and correct effectively errors arising in the code matrix Y [4, 5]. Also in the works [6, 7] the so-called "golden" cryptography based on the "golden" matrices was developed.

The main purpose of the present article is to generalize a matrix approach to cryptography and develop the so-called *matrix cryptography* based on special kind of square matrices – *non-singular matrices*. This kind of cryptography can be useful for digital signals used widely in media products operating in real scale of time, namely, sound signals, digital movies, cell telephone, audio and video players and so on.

2. Non-singular matrices

2.1. ***A definition and general properties of non-singular matrices.*** The Fibonacci matrices given by (2), (4), (6), (7), (8) and (10) have unique mathematical properties (5) and (11), that is, their determinants are equal only to (+1) or (-1). Also this means that these matrices are examples of more general class of square matrices called *non-singular matrices.* It is known that a square matrix A is called *non-singular*, if its determinant is not equal to zero [11], that is

$$\det A \neq 0. \qquad (12)$$

In linear algebra the non-singular matrices are called *invertible* because every non-singular matrix A has *inverse matrix* A^{-1}, which is connected with the matrix A with the following correlation:

$$AA^{-1} = I_n, \qquad (13)$$

where I_n is identity ($n \times n$)-matrix.

2.2. ***Non-singular (2×2)-matrices.*** Fibonacci Q-matrix (2) is a very special case of the non-singular (2×2)-matrices. The results for Fibonacci Q-matrix can be generalized to be used with all (2×2)-matrices. Let us consider a square non-singular (2×2)-matrix

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \qquad (14)$$

where $a_{11}, a_{12}, a_{21}, a_{22}$ are some real numbers. It is clear that the determinant of the matrix A is equal:

$$\det A = a_{11}a_{22} - a_{12}a_{21} \neq 0. \qquad (15)$$

Inversion of this matrix can be done easily as follows [11]:

$$A^{-1} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}^{-1} = \frac{1}{\det A} \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix} \qquad (16)$$

As is well known, determinant of a square matrix equals to the product of its *eigenvalues* [11]. Remind that the *eigenvalues* of the matrix (14) can be obtained as follows. Let us consider a square (2×2)-matrix constructed from the matrix (14):

$$A-\lambda I=\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}-\lambda\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}=\begin{pmatrix}a_{11}-\lambda & a_{12}\\ a_{21} & a_{22}-\lambda\end{pmatrix}, \qquad (17)$$

where I is an identity (2×2)-matrix and λ is continuous variable.

Determinant of the matrix (17) is called *characteristic polynomial* of the matrix A:

$$\det(A-\lambda I)=(a_{11}-\lambda)(a_{22}-\lambda)-a_{12}a_{21}=\lambda^2-(a_{11}+a_{22})\lambda+(a_{11}a_{22}-a_{12}a_{21}). \qquad (18)$$

Notice that the characteristic polynomial (18) can be written in terms of the trace $\mathrm{tr}(A)=a_{11}+a_{22}$ and the determinant $\det(A)=a_{11}a_{22}-a_{12}a_{21}$ of the matrix A as follows:

$$\det(A-\lambda I)=\lambda^2-\mathrm{tr}(A)\lambda+\det(A) \qquad (19)$$

It follows from the polynomials (18) and (19) a *characteristic equation* of the matrix A

$$\lambda^2-(a_{11}+a_{22})\lambda+(a_{11}a_{22}-a_{12}a_{21})=\lambda^2-tr(A)\lambda+\det(A)=0 \qquad (20)$$

Two roots of the equation (20)

$$\lambda_{1,2}=\frac{a_{11}+a_{22}}{2}\pm\sqrt{\frac{(a_{11}+a_{22})^2}{4}+a_{12}a_{21}-a_{11}+a_{22}}=\frac{1}{2}\left[\mathrm{tr}(A)-4\det(A)\right] \qquad (21)$$

is called *eigenvalues* of the matrix *A.*

Assume that a square (2×2)-matrix A (14) has two distinct eigenvalues λ_1 and λ_2. Using Lagrange Interpolation formula or Spectral Resolution of A, real power p of A can be calculated as follows:

$$A^p=\frac{A-\lambda_2 I}{\lambda_1-\lambda_2}\lambda_1^p+\frac{A-\lambda_1 I}{\lambda_2-\lambda_1}\lambda_2^p=\frac{1}{\lambda_1-\lambda_2}\left[(A-\lambda_2 I)\lambda_1^p-(A-\lambda_1 I)\lambda_2^p\right] \qquad (22)$$

This implies that elements of any real power of a (2×2)-matrix with distinct eigenvalues, is a linear combination of the same power of its eigenvalues. The coefficients in these linear combinations are constant and independent on real number p. This is a generalized form of *Lagrange Interpolating Polynomials*. Also it is referred as *Spectral Analysis* [] or *Spectral Resolution* of square matrices.

For example, the eigenvalues of Fibonacci Q-matrix (2) are

$$\lambda_1=\tau=\frac{1+\sqrt{5}}{2}\ \text{and}\ \lambda_2=-\frac{1}{\tau}=\frac{1-\sqrt{5}}{2}, \qquad (23)$$

where τ is the well-known golden mean. Obviously following equality can be written:

$$\det Q=\lambda_1\lambda_2=-1. \qquad (24)$$

According to (22), real power p of the Fibonacci Q-matrix can be calculated by

$$Q^p=\frac{1}{\sqrt{5}}\left[\left(Q+\frac{1}{\tau}I\right)\tau^p-(Q-\tau I)\left(-\frac{1}{\tau}\right)^p\right]$$

$$=\frac{1}{\sqrt{5}}\begin{pmatrix}\tau^{p+1}-\left(-\frac{1}{\tau}\right)^{p+1} & \tau^p-\left(-\frac{1}{\tau}\right)^p\\ \tau^p-\left(-\frac{1}{\tau}\right)^p & \tau^{p-1}-\left(-\frac{1}{\tau}\right)^{p-1}\end{pmatrix}. \qquad (25)$$

It is known that the *n*-th Fibonacci number can be expressed as *Binet formula* [8]:

$$F_n=\frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n-\left(\frac{1-\sqrt{5}}{2}\right)^n\right]. \qquad (26)$$

So (25) can be written in the form of

$$Q^p = \begin{pmatrix} F_{p+1} & F_p \\ F_p & F_{p-1} \end{pmatrix}. \quad (27)$$

2.3. General Square Matrices. Eq. (22) can be generalized to all square matrices of arbitrary size, with distinct eigenvalues. Let A to be a $(m \times m)$ square matrix with distinct eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_m$. Real power p of matrix A, can be calculated by

$$A^p = \sum_{i=1}^{m} \phi_{A,i}(A) \lambda_i^p \quad (28)$$

The matrix function $\phi_{A,i} : \mathbb{C}^{m \times m} \to \mathbb{C}^{m \times m}$ is defined by

$$\phi_{A,i}(X) = \prod_{\substack{j=1 \\ j \neq i}}^{m} \frac{X - \lambda_j I}{\lambda_i - \lambda_j}, \quad (29)$$

where $\mathbb{C}^{m \times m}$ denotes the set of $m \times m$ complex matrices and $X \in \mathbb{C}^{m \times m}$. This is a more general case of Lagrange Interpolating Polynomials and Spectral Analysis of square matrices. Setting $m = 2$ in (28) yields (22). These equations can be used to calculate any real power of any square matrix with distinct eigenvalues. Also these equations can be generalized to use with square matrices with repeated eigenvalues [?]. In the repeated eigenvalues case, $\phi_{A,i}$ is not independent on power p and varies for different values of power.

2.4. ***Jordan Matrix Decomposition***. Another way to calculate the real power of square matrices is based on *Jordan Matrix Decomposition*. Jordan decomposition of matrix A is written as

$$A = TJT^{-1} \quad (30)$$

where J is in Jordan canonical form, T is square matrix, whose columns are eigenvectors or generalized eigenvectors of A, and T^{-1} denotes the inverse of matrix T. In a more specific case, if $\lambda_1, \lambda_2, \ldots, \lambda_m$ are distinct eigenvalues of A, then Jordan canonical form of A is defined by

$$J = \begin{pmatrix} \lambda_1 & 0 & 0 & 0 \\ 0 & \lambda_2 & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & \lambda_m \end{pmatrix} \quad (31)$$

To calculate real power p of A, the following formula can be used:

$$A^p = TJ^pT^{-1} \quad (32)$$

This equation requires J^p to be calculated. Matrix J is diagonal, so calculation of its powers is very simple. Its real power p can be calculated as

$$J^p = \begin{pmatrix} \lambda_1^p & 0 & 0 & 0 \\ 0 & \lambda_2^p & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & \lambda_m^p \end{pmatrix} \quad (33)$$

and then as

$$A^p = T \begin{pmatrix} \lambda_1^p & 0 & 0 & 0 \\ 0 & \lambda_2^p & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & \lambda_m^p \end{pmatrix} T^{-1} \quad (34)$$

Eqs. (20) and (34) can be used to calculate any real power of any square matrix with distinct eigenvalues. Also there exist general versions of these equations, for repeated eigenvalue cases. For cryptographic applications, matrices with distinct eigenvalues are sufficient. So the repeated eigenvalue cases were not discussed in this section.

2.5. ***Non-singularity of powers.*** According to the previous sub-sections, determinant of a real power of a matrix can be computed using the following identity:

$$\det\left(A^{p}\right)=\det\left(A\right)^{p} \tag{35}$$

So if A is non-singular, any real power of this matrix is non-singular, too. In other word, non-singularity of matrix A or equivalently

$$\det\left(A\right)\neq 0 \tag{36}$$

implies that

$$\det\left(A\right)^{p}=\det\left(A^{p}\right)\neq 0 \tag{37}$$

So clearly A^{p} is not singular, too. This lemma is a basic assumption in the theory of Matrix Cryptography.

3. Matrix Approach to Cryptography

3.1. ***A general principle of a matrix approach.*** Let us consider a non-singular matrix E and its inverse matrix E^{-1}, which are connected by the identity (13). Now let us consider a square matrix X with the same size as the matrix E. Then we can write a product of the matrices E and X as follows:

$$Y = E\times X \tag{38}$$

If we multiply a matrix Y by an inverse matrix E^{-1}, we get:

$$E^{-1}\times Y = E^{-1}\times\left(E\times X\right)=\left(E^{-1}\times E\right)\times X = I\times X = X \tag{39}$$

The identities (28) and (39) give some *general principle*, which can be used in coding theory and cryptography. For the first time, this principle was formulated in the book [4].

Consider sequence $\left\{x_i\right\}_{i=1}^{N}$ which represents one-dimensional digital signal. The elements of this sequence can be rearranged in the form of $m\times m$ matrices. The result is a sequence of square matrices:

$$\begin{pmatrix} x_1 & \cdots & x_m \\ \vdots & \ddots & \vdots \\ x_{m^2-m+1} & \cdots & x_{m^2} \end{pmatrix},\begin{pmatrix} x_{m^2+1} & \cdots & x_{m^2+m} \\ \vdots & \ddots & \vdots \\ x_{2m^2-m+1} & \cdots & x_{2m^2} \end{pmatrix},\ldots \tag{40}$$

Element of this new sequence are defined by:

$$X_k=\begin{pmatrix} x_{(k-1)m^2+1} & \cdots & x_{(k-1)m^2+m} \\ \vdots & \ddots & \vdots \\ x_{km^2-m+1} & \cdots & x_{km^2} \end{pmatrix} \tag{41}$$

The sequence of square matrices $\left\{X_k\right\}_{k=1}^{K}$ contains the same data as sequence $\left\{x_i\right\}_{i=1}^{N}$. To encrypt the sequence $\left\{x_i\right\}_{i=1}^{N}$, it can be reformed to build a sequence of square matrices. Suppose that $\left\{E_k\right\}_{k=1}^{K}$ is a sequence of non-singular square matrices of the same size of X_k. Multiplication of E_k and X_k yields:

$$Y_k = E_k X_k \tag{42}$$

and thus the sequence of $\left\{Y_k\right\}_{k=1}^{K}$ is defined. Inverting the operations done in Eq. (39) to create matrix sequence $\left\{X_k\right\}_{k=1}^{K}$, the matrix sequence $\left\{Y_k\right\}_{k=1}^{K}$ is transformed into scalar sequence $\left\{y_i\right\}_{i=1}^{N}$. This new sequence is an encrypted form of original sequence $\left\{x_i\right\}_{i=1}^{N}$. The cryptographic key, which is used here, is the sequence of non-singular matrices $\left\{E_k\right\}_{k=1}^{K}$. Some methods for defining this Encoder Sequence of non-singular matrices are discussed in the followings sub-sections.

3.2. ***Matrix Cryptography for Digital Sound Signals.*** One possible way to define non-singular matrices in the encoder sequence is to define these matrices as real powers of a non-singular matrix, namely *Kernel* matrix. Assume that B is a non-singular matrix. According to sub-section 2.5, all real

powers of matrix B are also non-singular. So real powers of this matrix can be used to create a sequence of non-singular matrices, and this is all needed to define an encoder sequence. Assume that encoder sequence is in the form of $\{E_k\}_{k=1}^{K}$. Suppose $\{p_k\}_{k=1}^{K}$ to be a sequence of real numbers. Then elements of the encoder sequence can be defined by:

$$E_k = B^{p_k}, \tag{43}$$

which is the definition of encoder sequence as real powers of a non-singular kernel matrix B.

Digital sound signal is an example of one-dimensional data signals. Note that if the signal is recorded in multi-channel mode, any channel of this sound is one-dimensional. In this sub-section, a single channel of sound is argued and the cryptographic algorithm is applied to a single channel. Digital sound signals are saved and stored in many formats in the computers. Here the algorithm is applied to sounds with Microsoft RIFF Wave format [?]. It is the main format used in Microsoft Windows systems, to store raw and usually uncompressed digital sounds. In this format, data existing in a physical sound is sampled at a constant frequency, called Sample Rate. Amplitude of samples is saved in the file as data, and later the sound will be played back by audio hardware. When all amplitudes of sound are multiplied or divided by a constant, the volume of sound is the only thing which is changed. While the relative value of amplitudes remains unchanged, the sound is same. Since the value of amplitudes have to lie in the range of $[-1,1]$, all sounds in the algorithm are normalized to have largest absolute value of amplitudes, equal to 1.

Suppose $x[n]$ is a digital signal, and represents a digital sound, which is sampled at 22 kHz and Mono. The plot of this sound is shown in Fig. 1. This signal can be represented is the sequence form as $\{x_i\}_{i=1}^{N}$.

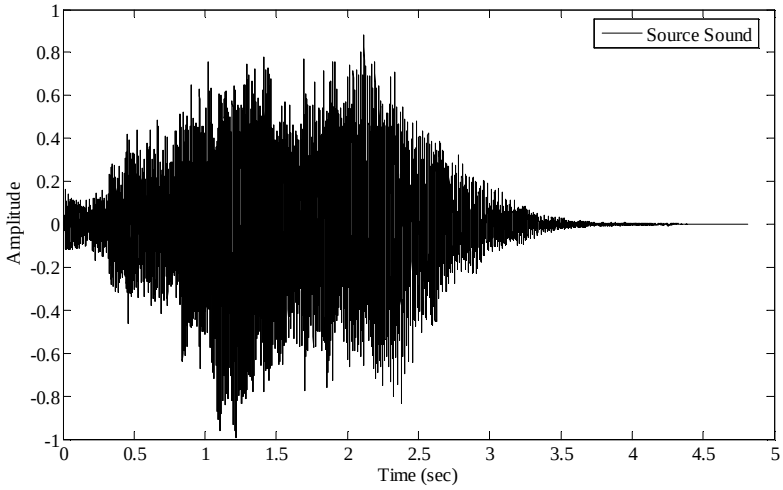


Figure 1. A sample digital sound signal

To apply the matrix cryptography to this signal, the following non-singular matrix is used as kernel:

$$B = \begin{pmatrix} 0.2 & -1 \\ 1 & -0.5 \end{pmatrix} \tag{44}$$

The powers of this matrix are computed where powers are real numbers, in the range of [-5, 5]. The power variable is referred as p. Elements of resulting matrices are functions of p. They are sketched and shown in Fig. 2. The values 1, 0 and -1 for p, correspond to B, 2×2 identity and inverse of B, respectively. In fact, Fig. 2 shows infinite number of non-singular matrices, suitable to be used as elements of encoder sequence. Here these matrices are used as encoders, and the Matrix Cryptography is applied on a sample digital sound signal.

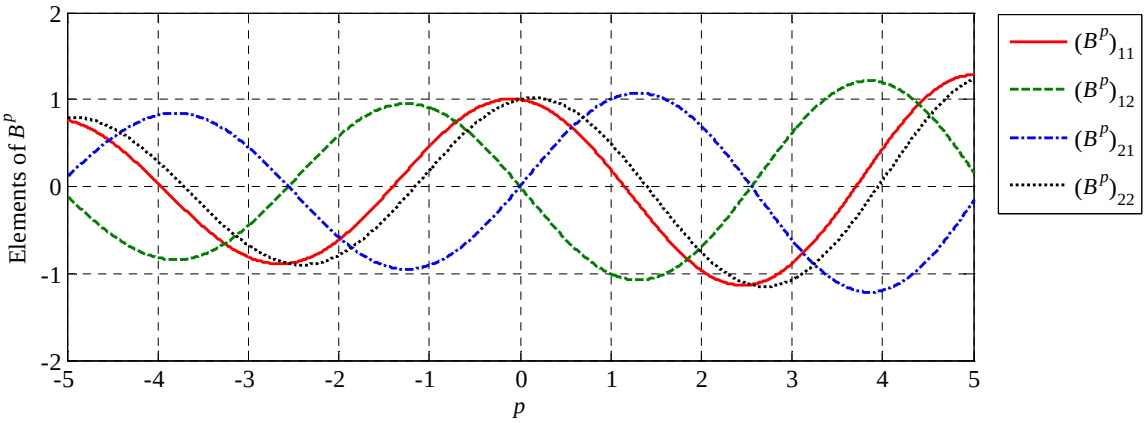


Figure 2. Real powers of matrix B in the range [-5, 5]

According to size of B, the elements of sequence $\{x_i\}_{i=1}^{N}$, corresponding to the sample sound shown in Fig. 1, must be reformed to build a sequence of 2×2 square matrices, like $\{X_k\}_{k=1}^{K}$. N and K are appropriate numbers and in the case of this problem, $N=4K$. The elements of power sequence $\{p_k\}_{k=1}^{K}$, are generated randomly with a uniform distribution over the range [-5, 5]. The sequence of encoder matrices $\{E_k\}_{k=1}^{K}$, is calculated by the rule $E_k = B^{p_k}$. Encrypted matrix sequence $\{Y_k\}_{k=1}^{K}$, is the element-by-element multiplication of the encoder sequence $\{E_k\}_{k=1}^{K}$ and data sequence $\{X_k\}_{k=1}^{K}$. Flattening the elements of matrix sequence $\{Y_k\}_{k=1}^{K}$, yields the numerical sequence of encrypted data $\{\hat{y}_i\}_{i=1}^{N}$. This sequence may assumed as a representation of a encrypted sound signal, which has the same duration as the original sound signal. As mentioned before, amplitude of digital sounds are bounded in the range [-1, 1], and the elements of $\{\hat{y}_i\}_{i=1}^{N}$ may not lie in this range. Hence, the sequence $\{\hat{y}_i\}_{i=1}^{N}$ must be normalized to obtain the sequence $\{y_i\}_{i=1}^{N}$. The elements of this sequence are defined by:

$$y_i = \frac{\hat{y}_i}{\max\limits_{1\le j\le N} \hat{y}_j} \qquad (45)$$

The resulting sequence represents a sound signal and is an encrypted form of the original sound signal. A graphical representation of the encrypted sound, is displayed in the Fig. 3. As it can be seen, the sound is normalized and has a maximum amplitude, equal to 1. The overall view of the original sound, shown in Fig. 1, and encrypted sound, shown in Fig. 2, is similar. To distinguish between them, a closer view of these sound are shown in Fig. 4. The time scope of these views, begins in second 2 with the length of 3 milliseconds.

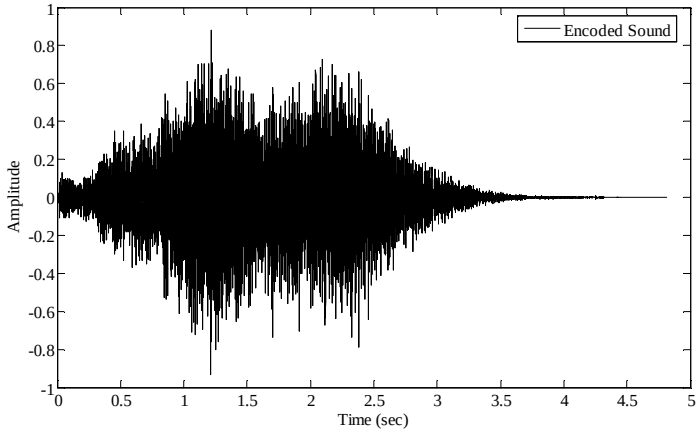
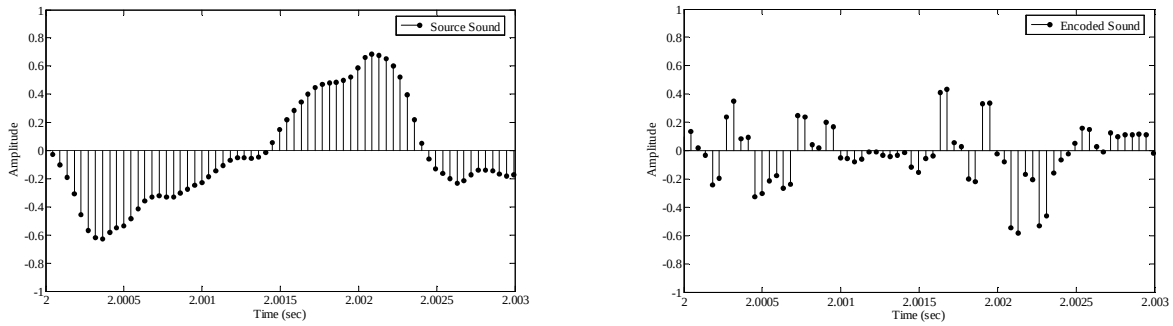


Figure 3. Encrypted form of the sound, shown in Fig. 1



(a) Original Sound (b) Encoded Sound

Figure 4. A closer view of the original and encrypted sound signals

Due to non-singularity of all encoder matrices, the original data can be recovered completely from the encrypted data. The decryption algorithm is just like the encryption algorithm. The only thing, which differs, is the sequence of powers. In the decryption phase, the negated form of power sequence of encryption phase must be used. The resulting sound signal after decryption of the encrypted sound signal is name Recovered Signal, hereafter. A block diagram of encryption and decryption phases is shown in Fig. 5. The input signal $x[n]$ is passed into an encryption process which yields encrypted signal $y[n]$. Also the latter signal is passed to a decryption process yielding the recovered signal $\hat{x}[n]$.

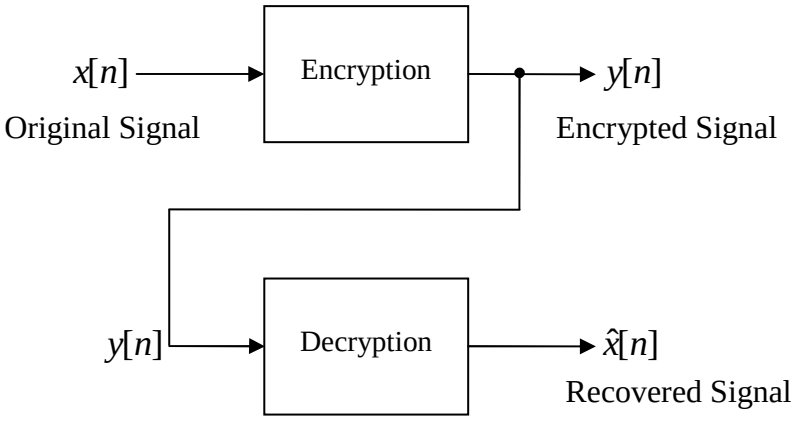


Figure 5. Block diagram of encryption and decryption processes

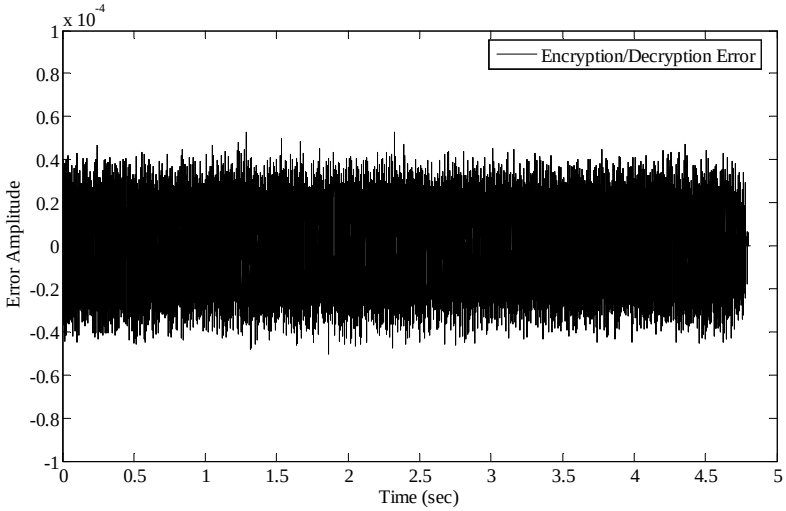


Figure 6. Encryption/Decryption Error for the algorithm applied on the signal shown in Fig. 1

As known, the binary representation, which is used in digital computers, can not represent all real numbers accurately and round-off error in not avoidable. The numbers appeared in this encryption/decryption algorithm, are real numbers in general and most of them can not be represented using finite number of bits. Because of the mentioned round-off error, the recovered signal and original signal are not equal necessarily and there exists an Encryption/Decryption Error in the algorithm. This error for the sample sound, shown in Fig. 1, corresponding recovered signal, is shown in Fig. 6. The maximum amplitude of this error is about 5×10^{-5}, which is very small in comparison with the original sound amplitude. This existence of this error is one of the limitations of the implementation of the matrix cryptographic algorithms in digital computers and restricts the application of this algorithm to the fields which not need exact recovery of encrypted data.

3.3. ***Matrix Cryptography for Images.*** In this sub-section application of Matrix Cryptography on digital images is discussed. Images are 2-dimensional signals and the digital image can be represented as a 2-dimensional sequence of color data. One of useful color coding approaches, used in digital computers, is RGB coding. This coding is based upon the fact that, every color can be represented as a linear combination of three base light beams: Red, Green and Blue. Digital images are saved in digital computers as 2-dimensional array of color data. Each element of this array is called Pixel. Every pixel in a digital image has a color, composed of three elements, red, green and blue. Each element of a color, in 24-bit color coding standard, has 8 bits of data. So the elements of a 24-bit RGB color are positive integer ranging from 0 to 255. It is usual to scale this range into the range of real numbers between 0 and 1. Decomposition of color of every pixel in a digital image, into corresponding red, green and blue elements, yields three numerical 2-dimensional arrays. Each of these array are in the form of $x[i, j]$ where $i = 1, 2, \ldots M$ and $j = 1, 2, \ldots, N$. M and N are vertical and horizontal size of picture respectively. It is assumed that values of elements of this array are normalized to be in the range [0, 1].

To apply matrix encryption on a sample image, the method of previous sub-section is used to create encoder sequence. Note that, all sequences in this sub-section assumed to be 2-dimensional and have appropriate size and number of elements. The kernel matrix which is used in this sub-section is:

$$B = \begin{pmatrix} 0.2 & -1 & 0 & 0.1 & 0.3 & 0 & 0 & 0.2 \\ 1 & -0.5 & -0.1 & 0 & 0 & -0.7 & -0.2 & 0 \\ 0 & -0.2 & 0.3 & -1 & 0 & -0.1 & 0.1 & 0 \\ 0.2 & 0 & 1 & 0.6 & 0.1 & 0 & 0 & 0.5 \\ 0.3 & 0 & 0 & 0.1 & 0.1 & -1 & 0 & 0.1 \\ 0 & -0.8 & -0.1 & 0 & 1 & -0.5 & -0.1 & 0 \\ 0 & -0.2 & 0.2 & 0 & 0 & -0.2 & 0.2 & -1 \\ 0.2 & 0 & 0 & 0.5 & 0.2 & 0 & 1 & 0.4 \end{pmatrix} \tag{46}$$

This matrix is non-singular and has non-negative eigenvalues. So all of its real powers are real matrices and can be used as encoder matrices. To use this matrix as a kernel, the data in the original image must be reformed into 8×8 matrices. Simply, the original image is divided to 8×8 image blocks and the corresponding data for each block is used to create the source matrix sequence. The sequence of powers is generated as a random variable, uniformly distributed in the range [-10, 10]. Some of elements of real powers of the matrix B in this power range, are displayed in Fig. 7. The algorithm, using the matrix (46) as kernel, is applied to the image shown in Fig. 8-(a). The Encrypted algorithm is shown in Fig. 8-(b). If the encrypted image is decrypted, the yields the recovered image which is shown in Fig. 8-(c). It can be seen that, the recovered image is very similar to the original image and the probable errors are negligible. The errors are due to round-off and limitations in binary representations, which is discussed in previous sub-section. Some other experimental results are shown in Fig. 9. Matrix cryptography is applied to several images and then recovered back. The kernel of all experiments is same, as defined in Eq. (43).

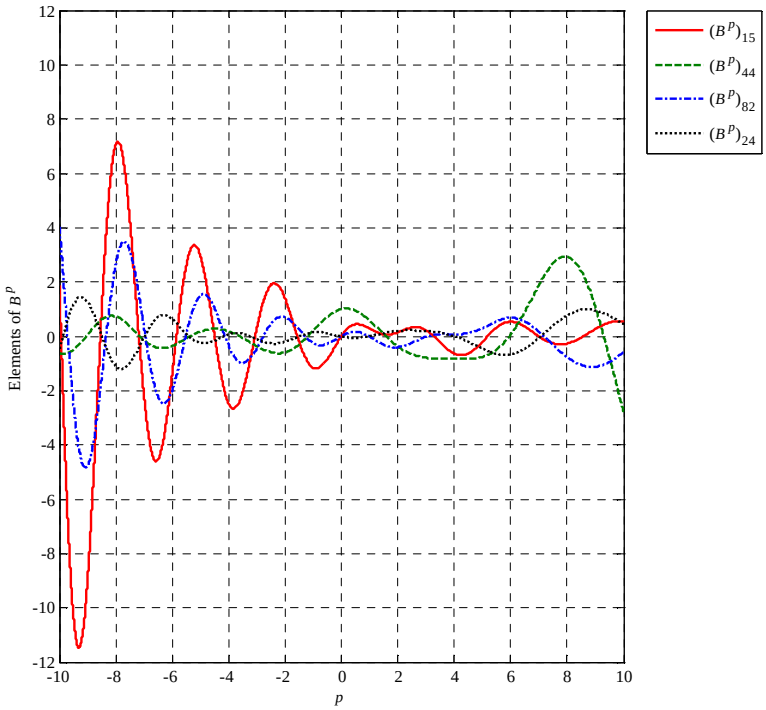


Figure 7. Some elements of the real powers of matrix B , defined in Eq. (103) in the range [-10, 10]

(a) Original image

(b) Encrypted image

(c) Recovered image

Figure 8. The matrix cryptography is applied on image (a) and the image (b) is obtained. Image (b) is an encrypted form of (a). If the image (b) is decrypted, image (c), the recovered image, is obtained.

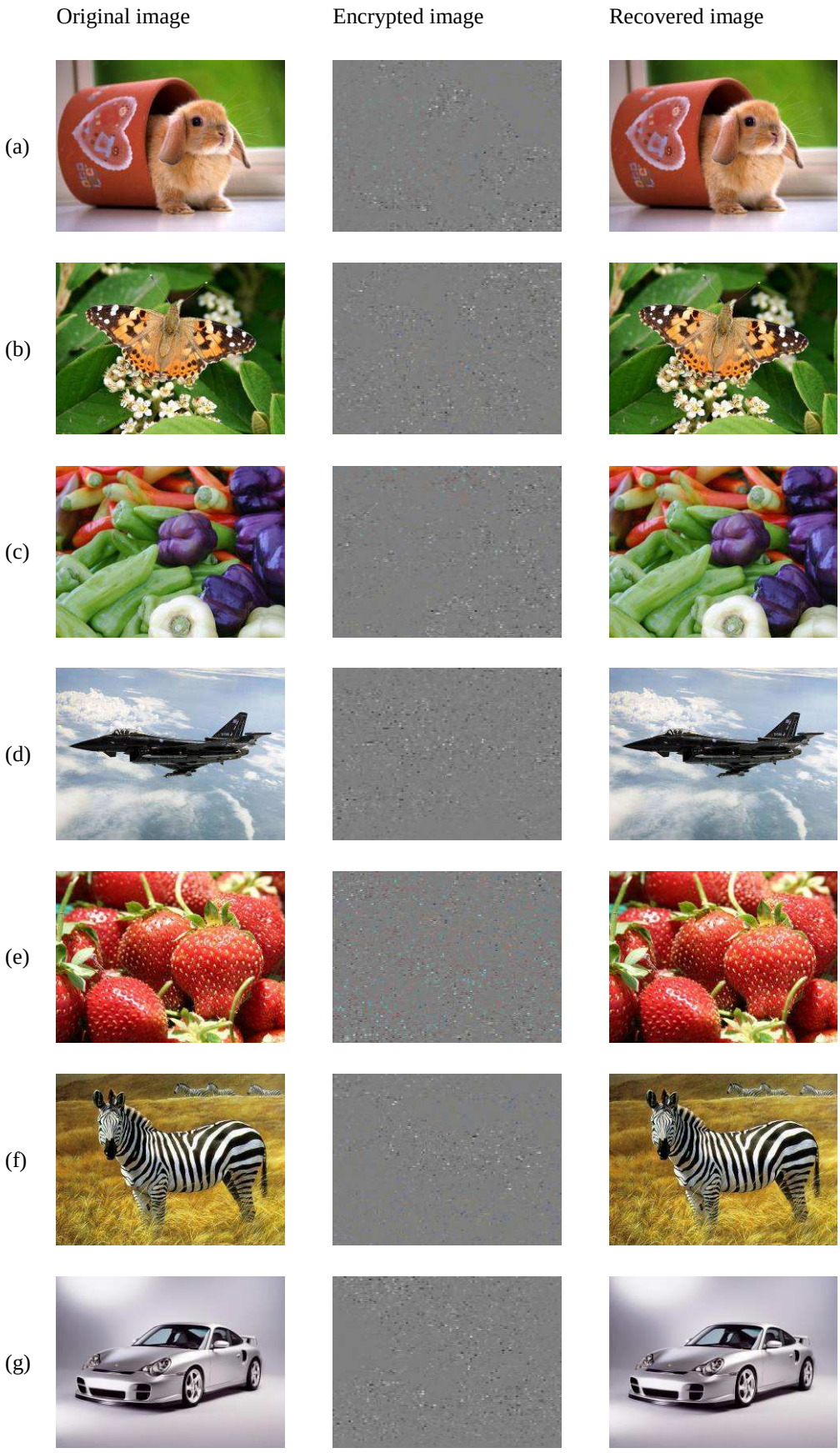


Figure 9. Some additional experimental results for Matrix Cryptography application for images

4. Conclusion

Thus, the main result of this study is an elaboration of new cryptographic method based on matrix approach (matrix cryptography). Digital signals (including digital sound signals and digital images), which are used widely in modern media products, are real area of application of the matrix cryptography. This method refers to symmetric-key cryptography. As cryptographic key, the method uses special kernel matrix, which is non-singular matrix, and some real number p, which is used as a power of the kernel matrix. In order to transmit cryptographic key from Sender to Receiver, we can use public-key cryptosystem. In order to protect this method from cryptographic attacks we can use a method of fast change of random cryptographic keys transmitted by public-key cryptosystem. Matrix cryptography can be used effectively for protection of digital music and digital movies from forbidden access.

References:

1. Diffie W. and Hellman M. E. New Directions in Cryptography. IEEE Trans. on Info. Theory, Vol. IT-22, 644-654 (1976).
2. Mollin, Richard A. *An Introduction to Cryptography*. Second Sedition: CRC, Champan & Hall, 2001.
3. Hybrid cryptosystems. From Wikipedia, the free encyclopedia. http://en.wikipedia.org/wiki/Hybrid_cryptosystem
4. Stakhov A, Massingue V, Sluchenkova A. Introduction into Fibonacci coding and cryptography. Kharkov: Publishing House "Osnova", 1999.
5. Stakhov A. Fibonacci matrices, a generalization of the "Cassini formula," and a new coding theory. *Chaos, Solitons & Fractals*, 2006, Volume 30, Issue 1, 56-66.
6. Stakhov AP. The **"**golden**"** matrices and a new kind of cryptography. *Chaos, Solitons & Fractals*, 2007, Volume 32, Issue 3: 1138-1146.
7. Stakhov A.P. Gazale formulas, a new class of the hyperbolic Fibonacci and Lucas functions, and the improved method of the "golden" cryptography. Moscow: *Academy of Trinitarism*, http://www.trinitas.ru/rus/doc/0232/004a/02321063.htm № 77-6567, publication 14098, 21 December, 2006.
8. Hoggat V.E. Jr. *Fibonacci and Lucas Numbers.* Boston: Houghton Mifflin, MA, 1969.
9. Stakhov AP. A generalization of the Fibonacci *Q*-matrix. *The journal "Reports of the National Academy of Sciences of Ukraine"*, 1999, No 9, 46-49.
10. Stakhov AP. Introduction into algorithmic measurement theory. Moscow: Publishing House "Soviet Radio", 1977 (in Russian).
11. Invertible matrices. Wikipedia. Free Encyclopedia http://en.wikipedia.org/wiki/Invertible_matrix