Information Sciences Letters
An International Journal

http://dx.doi.org/10.18576/isl/050301

Multi-Service Data Security Algorithm Based on Substitution Ciphers and Hadamard Transform

*Marghny H. Mohamed and T. A. Tammam**

Department of Computer Science, Faculty of Computers and Information, Assiut University, Egypt

Received: 3 Jun. 2016, Revised: 20 Aug. 2016, Accepted: 28 Aug. 2016
Published online: 1 Sep. 2016

Abstract: Cryptography has attracted much attention of many researchers, especially in protecting signal information as a part of an information security system. Several types of research have been done in developing too many approaches with the main focus on confidentiality of the Cryptography framework. “Golden” Matrices Cryptography (GC) has demonstrated superior performance compared to the state-of-the-art algorithms in terms of the computational time. However, it sometimes shows unsecured performance due to easily guess the encryption key. In this paper, an approach to overcome the main limitation of GC by a combination of N-Blocks Random Matrix ASCII Ciphers (NBRMAC), Hadamard product of Golden matrices and Hadamard Transform is proposed. Message Authentication Code (MAC) will be considered in the process to provide authentication and integrity. The proposed scheme is implemented out of the seven stages, starting with encoding plaintext by (NBRMAC) , applied HMAC, key generation, encryption stage, decryption stage, matching HMAC, and finally the decoding to obtain the original data at the end of communication.

Keywords: Computer Security, Cryptography, Golden matrices, Fibonacci numbers, Hadamard Product, Hadamard Transform, HMACs

1 Introduction

The transfer of information over the Internet has become more prevalent than ever before in order to provide Internet services over the world. But this leads to an increase in the risks and the attacks became large than any time. So we must protect transmitted information in order to acquire preserving the integrity, authentication, and confidentiality of information, including hardware, applications, confidential information like e-commerce, user-names, passwords, emails contents, banking, corporate information, and online transaction processing applications, and etc., which is exposed to unauthorized access. In order to keep the information and prevent unauthorized user from accessing the data, a variety of techniques have been proposed. Steganography and cryptography are the main methods of these techniques. Steganography is the art of covered or hidden writing, which hides the secret data into multimedia data such as sounds, images or videos [1]. The art of covered or hidden writing is called steganography which hides the existence of the message. The Greek words steganos and graphia are the radix of the word Steganography and it means “hiding writing” [2,3,4,5,6,7,8]. On the other hand, Cryptography is defined in the Oxford Dictionary as ”art and science of writing or solving codes”. This process utilizes mathematical algorithms to protect data based on keys, which encrypt the data (plaintext) into a ciphertext using encryption algorithms, and no one can decrypt the secret message and gets the original message (plaintext) except the user who has the keys [9].
In essence, the primary objectives of cryptography is to provide four fundamental information security services.

1. **Confidentiality:** “Assures that private or confidential information is not made available or disclosed to unauthorized individuals” [10].
2. **Integrity:** “Assures that information and programs are changed only in a specified and authorized manner” [10].
3. **Non-repudiation:** Assures that the sender actually sent the message, and can’t deny creating or sending the message. On the other hand, the recipient cannot claim that he does not receive the message [2].
4. **Authentication:** is a service which provides the identification of the sender and recipient. And also is applied to both the entity and the message. Where

* Corresponding author e-mail: TammamAli@fci.au.edu.eg

used to identify the sender and ensure received the message from the sender [11].

Cryptography is implemented into two kinds of key-based algorithms: symmetric key encryption (secret-key ciphers) and asymmetric key encryption (public-key ciphers). Asymmetric key encryption is a cryptography process that has two different keys (private and public), use the public key in the encryption process and private key in decryption process. Because users use two keys, the public key is known to any one and private key which is known only to the user. There is no need for distributing them prior to transmission [12]. Symmetric key encryption is an algorithm that uses the same key for encrypting and decrypting data, so the key must be shared over a secure channel before the communication [9] as Shown in Fig.1.

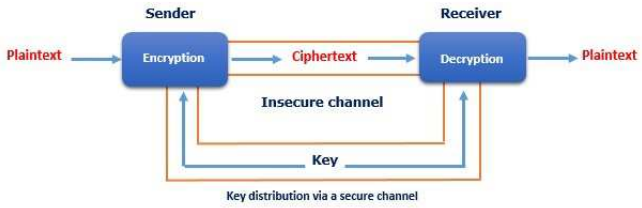

Fig. 1: Encryption /Decryption process.

Symmetric key encryption is represented in two forms: Block Cipher and Stream Cipher. A Block Cipher is a method of encryption that divides the plaintext into equal blocks, then encrypted each block individually and collect these blocks which represent ciphertext at the end[12]. Stream Cipher is a method of encryption that encrypt the plaintext as a stream of bits individually. This is achieved by encrypting the stream of bits sequentially using some of the results from the previous bit until all the bits in the data are encrypted as a whole using a time-varying transformation. Id is deduced that symmetric-key cipher algorithms are almost 1000 times faster than asymmetric-key cipher algorithms [12].

The substitution cipher is one of the classical encryption techniques which encode the letters of plaintext according to a special mechanism. This method can be done by replacing letters of the message with other letters, numbers, or symbols. This message also can be implemented by replacing single, or couple, or triplets of letters, and so on. The original message can be obtained by performing inverse substitution process [10].

Many algorithms have been demonstrated to utilize the cryptography. The (GC) “Golden” cryptography is one of the most important considerations of cryptography algorithms. Several types of research have been focused on increase improving the performance of the (GC) method to be more secure.

A.P. Stakhov, deduced a new kind of cryptography based on Fibonacci Q-matrix for continuous domain called (GC) “Golden” cryptography and concluded that the “Golden” cryptosystems is fast, simple for technical realization and reliable cryptosystems for protection of digital signals used in telecommunication and measurement systems [13].

K.R. Sudha and A.Chandra S. and Prasad R. P V G D examines the application of recurrence relations in the continuous domain and a cryptographic method based on the recurrence relations [14]. They use Bernoulli numbers recurrence besides Fibonacci numbers, became the level of security is more since it involves three parameters i.e., the permutation, the power of the matrix and type of recurrence used.

Ayse N., did the generalization of Hadamard product of Fibonacci Q^n matrix and Fibonacci Q^{-n} for continuous domain [15].

Angel M. R. and Gerardo R. S., discovered that the security of ”Golden” cryptography which is trivially compromised as it does not pass one of the basic cryptanalytic attacks: the chosen plaintext attack [16].

Shaligram P. and Amber J. and Ramjeevan S. T., Proposed a new approach for information security using Fibonacci Q-Matrix and concluded that The GC algorithms work faster than other symmetric algorithms (including DES, 3DES, AES, and Blowfish) [17].

Background of the problem is shown in section 2. Section 3 introduces our proposed algorithms. Section 4 discusses the experimental results and finally states the conclusions in Section 5.

2 Background

2.1 Recurrence Relations:

Recurrence relation is defined in mathematics, as an equation that recursively defines a sequence or multidimensional array of values, once one or more initial terms are given, each further term of the sequence or array is defined as a function of the preceding terms. K.R. Sudha, et al., presented three recurrence relation Fibonacci, Lucas, and Bernoulli’s Numbers [14].

1. **Fibonacci Numbers** $\{F_n\}_{n=1}^{\infty}$**:** are the sequence of numbers $(1,1,2,3,5,8,13,21,34,...)$ defined by the

linear recurrence equation

$$F_{n+1} = F_{n-1} + F_n, n \geq 3 \tag{2.1}$$

with the initial

$$F_1 = F_2 = 1 \tag{2.2}$$

which the next number is found by adding up the two numbers before it.

2.**Lucas Numbers:** are the sequence of numbers $(2,1,3,4,7,11,...)$ the Lucas numbers L_k is defined by recurrence formula and initial terms as :

$$L_{k+1} = L_k + L_{k-1}, k \geq 1 \tag{2.3}$$

with

$$L_0 = 2, L_1 = 1. \tag{2.4}$$

3.**Bernoulli's Numbers:** the Bernoulli numbers B_n are a sequence of signed rational numbers that can be defined by the exponential generating function.

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!}, |x| < 2\Pi \tag{2.5}$$

with recursion formula is:

$$B_n = -\frac{1}{n+1} \sum_{k=0}^{n-1} \binom{n+1}{k} B_k, n \succeq 1 \tag{2.6}$$

where all numbers are zero with odd index n>1. The even-indexed numbers alternate in sign. Taking B_0 = 1, B_1 = -$\frac{1}{2}$, which successively yields the values $B_2 = \frac{1}{6}, B_4 = -\frac{1}{30}, B_6 = \frac{1}{42}, B_8 = -\frac{1}{30}, ...$

2.2 Fibonacci Q-matrix

A.P. Stakhov in [13,18] introduced the following square (2×2) matrix:

$$Q = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \tag{2.7}$$

and proved the following property of the nth power of the Q-matrix in [18]:

$$Q^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}, \tag{2.8}$$

$$Det Q^n = F_{n+1}.F_{n-1} - F_n^2 = (-1)^n, \tag{2.9}$$

where $n = 0, \pm 1, \pm 2, \pm 3, ..., F_{n-1}, F_n, F_{n+1}$ are Fibonacci numbers.

The Hadamard product is an entrywise multiplication of two matrices of the same dimensions, and generates matrix which inherits the same benefits of product [19]. For matrices A and B $(m \times n)$ matrices but not necessarily square, the Hadamard product of A and B given by

$$[A \circ B]_{ij} = [A]_{ij} [B]_{ij} \tag{2.10}$$

The Hadamard product of Fibonacci Q^n and Q^{-n} matrices are represented in following form:

$$Q^n \circ Q^{-n} = \begin{pmatrix} F_{n+1}F_{n-1} & -F_n^2 \\ -F_n^2 & F_{n+1}F_{n-1} \end{pmatrix}, \tag{2.11}$$

and the inverse of this matrix can be written as

$$(Q^n \circ Q^{-n})^{-1} = \begin{pmatrix} \frac{1+F_n^2}{1+2F_n^2} & \frac{F_n^2}{1+2F_n^2} \\ \frac{F_n^2}{1+2F_n^2} & \frac{1+F_n^2}{1+2F_n^2} \end{pmatrix}, \tag{2.12}$$

as described by [15,20].

2.3 Hadamard Matrices

A Hadamard matrix of order n is a matrix H_n with elements ± 1 such that

$$HH^T = nI_n, \tag{2.13}$$

where I_n is the $(n \times n)$ identity matrix and H^T is the transpose of H, that is for which the real inner product of any pair of distinct rows is 0 [21]. For examples in the case n = 1, 2, and 4 the Hadamard matrices are

$$H_1 = [1], H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}. \tag{2.14}$$

The Hadamard transform is a symmetric orthogonal matrix whose elements are real numbers 1 and -1 [22]. The normalized Hadamard matrices of order 2^n, denoted by H_n, is defined recursively in the following form:

$$H_1 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \tag{2.15}$$

$$H_{n+1} = \frac{1}{\sqrt{2}} \begin{bmatrix} H_n & H_n \\ H_n & -H_n \end{bmatrix}, n \geq 1. \tag{2.16}$$

2.4 The Fibonacci P-Numbers

For an integer $p = 0,1,2,...$ and $n \geq p+2$, the n^{th} Fibonacci P-numbers is formed by the recurrence relation [18,23].

$$F_p(n) = F_p(n-1) + F_p(n-p-1), \tag{2.17}$$

with initial terms:

$$F_p(1) = F_p(2) = ... = F_p(p) = F_p(p+1) = 1.$$

The Fibonacci p-numbers also extended to negative values of n. By taking $n = p+1$ in the recursion relation(13) we have

$$F_p(p+1) = F_p(p) + F_p(0).$$

The initial conditions are given by

$$F_p(p) = F_p(p+1) = 1, \text{ then } F_p(0) = 0.$$

As there are $p+1$ initial conditions for (13), we can use the same method to find the first p Fibonacci p-numbers for $n \leq 0$:

$$F_p(0) = F_p(-1) = F_p(-2) = ... = F_p(-p+1) = 0. \tag{2.18}$$

These are in essence the initial conditions for the negative Fibonacci p-numbers. Now, rearranging the recursion relation (13) gives $F_p(n-p-1) = F_p(n) - F_p(n-1)$. A shift by $p+1$ terms gives the following equivalent recursion relation:

$$F_p(n) = F_p(n+p+1) - F_p(n+p), n \leq -p. \tag{2.19}$$

This recursion relation and initial conditions (14) enable to find that:

$$F_p(-p) = F_p(1) - F_p(0) = 1. \tag{2.20}$$

Continuing the sequence gives:

$$F_p(-p-1) = F_p(-p-2) = ... = F_p(-2p+1) = 0. \tag{2.21}$$

and

$$F_p(-2p) = F_p(-p+1) - F_p(-p) = -1. \tag{2.22}$$

The generalized Fibonacci Q_p matrices were introduced in [18,24] by the following form:

$$Q_p = \begin{pmatrix} 1&1&0&0&\dots&0&0 \\ 0&0&1&0&\dots&0&0 \\ 0&0&0&1&\dots&0&0 \\ \vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots \\ 0&0&0&0&\dots&1&0 \\ 0&0&0&0&\dots&0&1 \\ 1&0&0&0&\dots&0&0 \end{pmatrix}. \tag{2.23}$$

where $p = 0,1,2,3,...$ and Q_p is a $(p+1)\times(p+1)$ square matrix as

$$Q_0 = (1), Q_1 = \begin{pmatrix} 1&1 \\ 1&0 \end{pmatrix}, Q_2 = \begin{pmatrix} 1&1&0 \\ 0&0&1 \\ 1&0&0 \end{pmatrix},$$

$$Q_3 = \begin{pmatrix} 1&1&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \\ 1&0&0&0 \end{pmatrix}, Q_4 = \begin{pmatrix} 1&1&0&0&0 \\ 0&0&1&0&0 \\ 0&0&0&1&0 \\ 0&0&0&0&1 \\ 1&0&0&0&0 \end{pmatrix}.$$

The n^{th} Power of the Q_P^n Matrix was introduced in [18, 24] as:

$$Q_P^n = \begin{pmatrix} F_p(n+1) & F_p(n) & \cdots & F_p(n-p+2) & F_p(n-p+1) \\ F_p(n-p+1) & F_p(n-p) & \cdots & F_p(n-2p+2) & F_p(n-2p+1) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ F_p(n-1) & F_p(n-2) & \cdots & F_p(n-p) & F_p(n-p-1) \\ F_p(n) & F_p(n-1) & \cdots & F_p(n-p+1) & F_p(n-p) \end{pmatrix}, \tag{2.24}$$

where $F_p(n)$ is Fibonacci p-number, $n = 0 \pm 1, \pm 2, \pm 3, ...$, and the matrix Q_3^n can be written as:

$$Q_3^n = \begin{pmatrix} F_3(n+1) & F_3(n) & F_3(n-1) & F_3(n-2) \\ F_3(n-2) & F_3(n-3) & F_3(n-4) & F_3(n-5) \\ F_3(n-1) & F_3(n-2) & F_3(n-3) & F_3(n-4) \\ F_3(n) & F_3(n-1) & F_3(n-2) & F_3(n-3) \end{pmatrix}, \tag{2.25}$$

where $n = 0 \pm 1, \pm 2, \pm 3, ...$ the determinate of the matrix $F_p(n)$ can be calculated using equation (22).

2.5 Hash-based Message Authentication Code HMAC

Message authentication code is the mechanism which is used between sender and recipient, to prove the integrity of a message which confirms that data received without any modification as sent. MAC (Message Authentication Code) is a technique which uses a secret key to generate a small fixed-length block of data for MAC that is sent with the message [25]. An HMAC (Hash-based Message Authentication Code) is a message authentication code that uses symmetric cryptographic key in involving with a hash function.

In our proposed we applied an HMAC function, to produce the MAC value by using Data Encryption Standard (DES) algorithm consists of the secret key and the message input, then send the MAC value to the receiver with the message. At the recipient side, computed the MAC value of the received message using the same key and HMAC function. Finally, the two MAC values are compared. In case of matching means, the message has been received correctly and ensuring that the sender who has shared the key.

3 The Proposed Schema

Data security algorithm is proposed. The key of encryption is changed from session to session for increasing the security, even if the cryptanalysis is getting the key of any session, it would be impossible to get the plaintext in next session.

The Golden cryptography algorithm is improved which became the security of algorithm based on the automatic key variability concept applied to the message based on recurrence relation functions by encoding the plaintext with generating N-Blocks Random ASCII Matrix Ciphers

(NBRMAC), applied Hadamard product of Fibonacci Q^n matrix and Fibonacci Q^{-n} matrix in first algorithm and applied Hadamard transform on Q^n matrix in the second algorithm.

3.1 N-Blocks Random Matrix ASCII Ciphers (NBRMAC) technique:

Assume the initial message is formed as a digital signal which can be represented in a vector as $P = \{a_1, a_2, a_3, \cdots, a_m\}$, where m is the length of the message. The message is divided into blocks, each block include letters from 1 to 2^{16}. The NBRMAC technique induces three stages key generation, coding the message, and decoding the message.

1.**Key Generation:**
This stage is divided into two steps:
(a)**Matrix Generation:** A matrix of order $(n \times n)$ blocks random matrices is generated, where n depends on the length of the block message (n= $ceil(\sqrt{m}$, ceiling functions return a real number to the smallest following integer [26]). Each block of the random matrix (BRM) as in (26) is constructed in (16×16) matrix of unique random ASCII. A very high range of key search space of order $((N \times N)! \times 256!)$ is generated which makes the matter more difficult to break the key.

$$BRM = \begin{bmatrix} A_{(0,0)} & A_{(0,1)} & A_{(0,2)} & \cdots & A_{(0,15)} \\ A_{(1,0)} & A_{(1,1)} & A_{(1,2)} & \cdots & A_{(1,15)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ A_{(15,0)} & A_{(15,1)} & A_{(15,2)} & \cdots & A_{(15,15)} \end{bmatrix}. \tag{3.1}$$

$$NBRMAC = \begin{bmatrix} BRM_{(0,0)} & BRM_{(1,0)} & BRM_{(0,2)} & \cdots & BRM_{(0,n)} \\ BRM_{(1,0)} & BRM_{(1,1)} & BRM_{(1,2)} & \cdots & BRM_{(0,n)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ BRM_{(n,0)} & BRM_{(n,1)} & BRM_{(n,2)} & \cdots & BRM_{(n,n)} \end{bmatrix}. \tag{3.2}$$

(b)Save the $(n \times n)$ blocks random matrices in the secret file as in (27).

2.**Coding the Message:**

(a)All characters of plaintext are converted into corresponding ASCII code, $P' = ASCII(P)$.
(b)The cipher vector $C = \{c_1, c_2, c_3, \cdots, c_n\}$ is created by replacing every element in vector P' with its corresponding cell in selected matrix (BRM). The process of substitution is done by finding the cell value of intersection of the row with column indexes in selected matrix (BRM), whereas search for the first element of P' in the first matrix (BRM), the second element of P' in the second matrix (BRM), and so on, in the case of access to the last matrix (BRM) and with not access the last element in P' starting again from the first matrix (BRM). The index of the row is calculated by computing the result of dividing the letter by the number sixteen, and the index of the column is also calculated by computing the remainder of dividing the letter by the number sixteen.
for k = 1 to n
$i = P'(k)/16$
$j = P'(k)\%16$
$C(k) = BRM_{(k)}(i, j)$

3.**Decoding the Message:**

(a)Read the random ASCII file in $(N \times N)$ blocks matrices, each matrix of order (16×16).
(b)Get the plaintext vector P by involves the inverse process of substitution. This process during search every element of ciphertext vector C in selected matrix (BRM) as encoding process, and return the row and columns indexes (I,J) and get the ASCII code for every element by multiplying the row index by number sixteen then add the column index to the result.
(c)All ASCII of plaintext are converted into corresponding characters, $P = String(ASCII(P'))$.

3.2 Algorithm 1:

Some steps will run at sender side:

1.**Encoding Stage:** By using N-Blocks Random Matrix ASCII Ciphers (NBRMAC) technique.
2.**Producing MAC Message:**
(a)Generate key by using DES Algorithm to compute an MAC over the encoding message and using HMAC function as (MAC1).
3.**Encryption Stage:**
(a)Input an encryption key parameters, K=(n,p,r), where (r is recurrence type, n represent recurrence order,and P order of fibonacci p-numbers).
(b)Construct the corresponding encryption matrix key E_p^n depending on the Hadamard product of Q_p^n and Q_p^{-n} matrices.
(c)Based on the value of (p), the encoding message C is split into blocks (**B**), each block contains $(p+1) \times (p+1)$ elements and represents into a square matrix.
(d)Compute the ciphertext $C_i = B_i \times E_p^n$ for each block of (B).
(e)Collect all encrypted blocks C_i into single vector.

Also, other steps will be done at the receiver side for decrypting a ciphertext, in addition to ensuring authenticity and message integrity according to the following stages:

1.**Decryption Stage:**
   (a)Load the ciphertext (C) into square matrices depending on (p) like in the encryption stage.
   (b)Compute the inverse of the Hadamard product of Q_p^n and Q_p^{-n} matrices in D_p^n.
   (c)For each block, compute $D_i = C_i \times D_p^n$.
   (d)Collect all decrypted blocks D_i into single vector(D).
2.**Verification stage:**
   (a)Compute MAC value of the obtained decryption of encoding message as (MAC2).
   (b)Compare (MAC1)and (MAC2), if it's matching, it means that the message is not modified over transmission.
3.**Decoding Stage:** by using N-Blocks Random Matrix ASCII Ciphers (NBRMAC) technique to get the plaintext.

3.3 Algorithm 2:

Some steps will run at sender side:

1.**Encoding Stage:** by using N-Blocks Random Matrix ASCII Ciphers (NBRMAC) technique.
2.**Producing MAC Message:**
   (a)Generate key by using DES Algorithm to compute an MAC over the encoding message and using HMAC function as(MAC1).
3.**Encryption Stage:**
   (a)Input an encryption key parameters, K=(n,p,h,r), where (r is recurrence type, n represent recurrence order, p order of fibonacci p-numbers,and h is Hadamard matrix order).
   (b)Construct the corresponding encryption matrix key E_p^n depending on the Hadamard transform of Q_p^n matrix.
   (c)Based on the value of (p), the encoding message C is split into blocks (**B**), each block contains $(p+1)\times(p+1)$ elements and represents in a square matrix.
   (d)Compute the ciphertext $C_i = B_i \times E_p^n$ for each block of (B).
   (e)Collect all encrypted blocks C_i into single vector.

Also, other steps will be done at the receiver side for decrypting a ciphertext, in addition to ensuring authenticity and message integrity according to the following stages:

1.**Decryption Stage:**
   (a)Load the ciphertext (C) into square matrices depending on (p) like in the encryption stage.
   (b)Compute the inverse of the Hadamard transform of Q_p^n matrix.
   (c)For each block, compute $D_i = C_i \times D_p^n$.
   (d)Collect all decrypted blocks D_i into single vector(D).
2.**Verification stage:**
   (a)Compute MAC value of the obtained decryption of encoding message as (MAC2).
   (b)Compare (MAC1)and (MAC2), if it's matching, it means that the message is not modified over transmission.
3.**Decoding Stage:** by using N-Blocks Random Matrix ASCII Ciphers (NBRMAC) technique to get the plaintext.

4 Experimental Results

For evaluation of the effectiveness of the proposed scheme. Twenty experiments were performed. These experiments were performed to evaluate system security by measuring the level of confusion and diffusion, by comparing relationship between the original messages and encryptions message using statistical methods.

Confusion and diffusion are two basic statistical criterias for cryptography algorithms. Diffusion is the process that tries to make the relationship between the plaintext and ciphertext are very intricate issue to prevent attempts to deduce the encryption key [10]. Confusion seeks for making the relation between the encrypted message and the key of encryption as complex as possible used [10].

Statistical analysis methods that will be used in our experiments are.

1.**The Correlation:** Used to measure the strength and direction of the linear relationship between two variables and is symbolized by a symbol (r) [27]. The value of the correlation r is always between +1 and -1.
2.**T-Test:** Used to know whether the two groups of numbers are statistically different from each other.

These factors used to test the proposed encryption algorithm properties (Confusion and diffusion). The correlation used between the pairs of values while paired t-test is used to test for differences in the mean values of each variable. If the value of Correlation equal:

1.1, this means the plaintext and the ciphertext are identical.
2.0, this means the plaintext and the ciphertext are different completely. It does mean encryption process is good.
3.-1, this means the ciphertext is the negative of the plaintext, which means the encryption process was successful.

In these experiments, different keys value and messages to prove the properties of the algorithms are used. The results are compare with more related algorithms like DES, TripleDES, Rijndael, Golden Cryptography using generalized Q_p (GCP), Golden Cryptography using n^{th} power of the Q_p^n matrix (GCPN), Golden Cryptography using Hadamard product of Q_p^n and

Q_p^{-n} matrices (GCPNH), and (c1m1, c1m2) [28].

The following three messages are used to test the proposed algorithms.

1. **Msg1:** cryptographist is the science of overt secret writing.
2. **Msg2:** meet me after the party meet me after the party.
3. **Msg3:** meet me after party.

We applied our proposed in the following steps:

1. Construct the plaintext vector for each message by replacing each character from message with its ASCII as follow:
   Msg1 = {67, 114, 121, 112, 116, 111, 103, 114, 97, 112, 104, 105, 115, 116, 32, 105, 115, 32, 116, 104, 101, 32, 115, 99, 105, 101, 110, 99, 101, 32, 111, 102, 32, 111, 118, 101, 114, 32, 115, 101, 99, 114, 101, 116, 32, 119, 114, 105, 116, 105, 110, 103, 46} as shown in figure(2)

2. **Encoding the message 1 by Algorithm (1)**
   Msg1 = {141, 137, 68, 220, 49, 179, 40, 242, 214, 230, 188, 200, 15, 204, 48, 148, 103, 3, 111, 181, 203, 148, 210, 20, 125, 73, 221, 5, 104, 58, 87, 163, 47, 165, 4, 74, 210, 71, 76, 126, 102, 177, 153, 233, 217, 127, 241, 209, 234, 61, 83, 145, 15, 31}

3. **Ciphertext of message 1 by Algorithm (1), with key parameters n=3, p=7, and r = fibonacci numbers**
   Msg1 = { 146, 167, 127, 141, 123, 27, 235, 245, 118, 154, 106, 214, 127, 25, 131, 191, 199, 77, 123, 103, 64, 48, 152, 175, 254, 119, 32, 125, 236, 214, 195, 230, 196, 249, 173, 47, 20, 70, 134, 174, 242, 40, 55, 102, 182, 11, 238, 71, 9, 234, 234, 234, 139, 226, 30 }

4. **Encoding the message 1 by Algorithm (2) Msg1** = {186, 126, 11, 182, 221, 208, 50, 111, 177, 222, 51, 231, 173, 105, 64, 119, 251, 124, 146, 63, 43, 69, 73, 107, 36, 25, 79, 35, 119, 127, 123, 211, 28, 90, 88, 14, 176, 75, 49, 232, 95, 38, 150, 199, 134, 172, 118, 43, 8, 186, 50, 237, 12, 5 }

5. **Ciphertext vector of Message 1 by Algorithm (2), with N=3, P=3, H=2, and r = fibonacci numbers**
   Msg1 = { 820.236, 1049.3364, 510.5262, 98.994, 1079.0346, 1196.4132, 554.3664, 431.331, 895.1886, 1595.2176, 428.5026, 301.2246, 914.9874, 782.0526, 398.8044, 128.6922, 1477.839, 704.2716, 503.4552, 261.627, 388.905, 595.3782, 18.3846, 43.8402, 376.1772, 205.059, -9.8994, 21.213, 852.7626, 1135.6026, 162.633, 60.8106, 367.692, 421.4316, -45.2544, 234.7572, 885.2892, 974.3838, 428.5026, -115.9644, 827.307, 724.0704, 56.568, -173.9466, 902.2596, 851.3484, 212.13, 425.6742, 175.3608, 1459.4544, -48.0828, 190.917, 50.9112, 21.213, 33.9408, 14.142 }

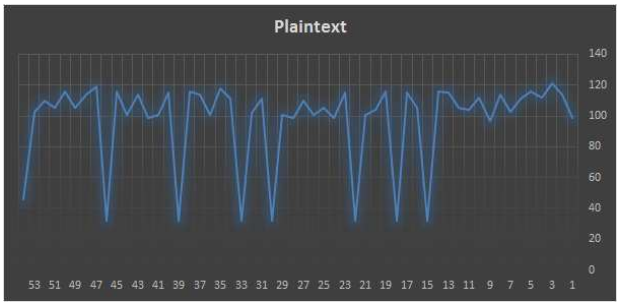

Fig. 2: Plaintext of Message 1.

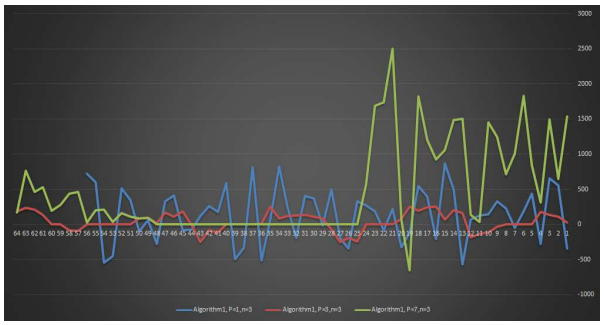

Fig. 3: Ciphertext of Message 1 Using Algorithm 1 in case of r = Fibonacci recurrence, n= 3 and p=(1,3,7)

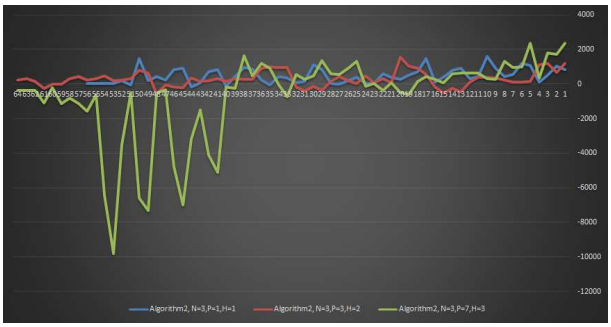

Fig. 4: Ciphertext of Message 1 Using Algorithm 2 in case of r = Fibonacci recurrence, n=3, p=(1,3,7), and h= 1,2,3

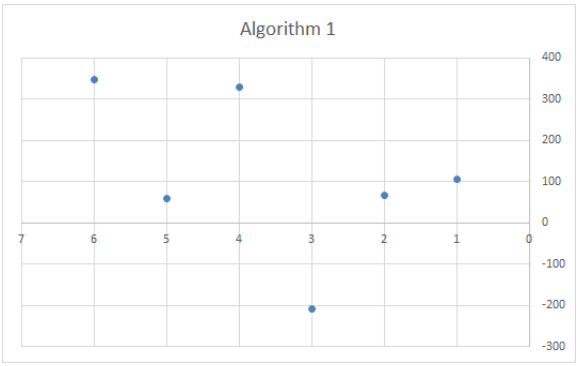

Fig. 5: Distribution of character 'i' of Message 1 Using Algorithm 1 in case of r = Fibonacci recurrence, n= 3, and p=1

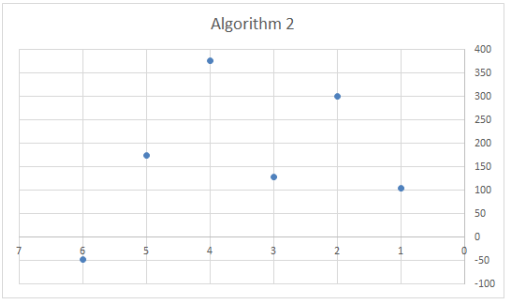

Fig. 6: Distribution of character 'i' of Message 1 Using Algorithm 1 in case of r = Fibonacci recurrence, n= 3, p=1 and h=1

Table 1: The Correlation from encryption messages

Algorithms	Correlation of Messages(Plaintext)		
	Message 1	Message 2	Message 3
DES	-0.0869411	0.0929350	0.1442248
TripleDES	-0.1731667	-0.1466628	0.2368577
Rijndael	0.2519883	-0.1193892	-0.1832509
GCP	0.1733070	0.3942284	0.0783463
GCPN	0.1296702	0.1031590	0.2267430
GCPNH	-0.1781493	-0.3144892	-0.3828152
C1m1	-	0.4011547	-
C1m2	-	0.2471558	-
Algorithm 1	-0.0465718	0.0666809	0.0391638
Algorithm 2	0.0487722	0.1163172	-0.0629608

From the resulted ciphertext we can clearly notice that the contrast between plaintext and ciphertext of messages 1, which are demonstrated in figures(3, 4) for each character on the plaintext message there is a different value appeared in the ciphertext, and there is no direct relationship between the plaintext and the ciphertext. This indicates that the proposed model has a high confusion because the relationship between the input key and the

Table 2: Paried t-test from encryption messages

Algorithms	Paried t-test of Messages(Plaintext)		
	Message 1	Message 2	Message 3
DES	0.0044	0.0052	0.0381
TripleDES	0.2798	0.0812	0.0259
Rijndael	0.0291	0.5412	0.1467
GCP	0.0001	0.0001	0.0001
GCPN	0.0001	0.0001	0.0001
GCPNH	0.0001	0.0001	0.0001
C1m1	0.0001	0.0001	0.0001
C1m2	0.0001	0.0001	0.0001
Algorithm 1	0.0001	0.0001	0.0001
Algorithm 2	0.0001	0.0001	0.0001

output message is nonlinear. And observe that it can generate ciphertext with the different values in every time with changing substitution technique if even using the same parameters of the key.

We observed that, message 1 has some repeated characters such as character 'i' for example repeated ten times, and every time the resulted cipher is different from others as shown in figures(5, 6). Its clear that the proposed model provides a high- level of diffusion.

The correlation coefficient values and paired t-test of the proposed encryption algorithm and other algorithms are shown in table 1 and table 2 respectively. In the case of ciphertext the values of the correlation coefficient of algorithm 1 range from (-0.0465718 to 0.0391638) and algorithm 2 range from (-0.0629608 to 0.0961064), which means that the plaintext and the ciphertext are different, so our proposed has provided a high confusion. The values of t-test shows that this difference is considered an extremely statistically significant, this means that the proposed encryption algorithm has a strong security.

Through the results, that were shown in the figures(3, 4, 5, 6) and values of correlation and t-test, The proposed cryptosystem has a high confusion and diffusion properties, which makes the cryptosystem of high key and plaintext sensitivity. Golden cryptography represents in the nonlinear equation, which makes the relationship between the plaintext, encryption key, and ciphertext nonlinear. This makes the possibility of retrieving any one of them impossible even if the others were known.

5 Conclusion

This paper provides multi-service data security including (confidentiality, authentication, and integrity). The encoding of the message by N-Blocks Random Matrix ASCII Ciphers (NBRMAC) technique provided a very high range of key search space. By using the key of the combination of (n^{th} Power of the Q_P^n matrix and discrete

Hadamard transform of Hadamard product of $Q_p^n \times Q_p^n$) provides Confusion and diffusion. Message authentication code (MAC) is employed for data authentication and integrity which constructed the digital signature of the scheme. The signed MAC and cipher are used for communication over computer networks. At the receiver end, after the decryption is done, the digital signature for encoding plaintext can be used to verify the integrity of the message, and the authentication of the sender then decoding the data to get the original data. The experimental results indicate that the proposed cryptosystem has a high confusion and diffusion properties, it has high security and it is suitable for secure communications.

References

[1] Marghny H. Mohamed and Loay M. Mohamed. High capacity image steganography technique based on lsb substitution method. *Applied Mathematics & Information Sciences*, 10(1):259–266, 2016.

[2] Naziha M. Al-Aidroos, Marghny H. Mohamed, and Mohamed A. Bamatraf. Data hiding technique based on dynamic lsb. *Naif Arab University for Security Sciences*, 2011.

[3] X. Liao, Q.Wen, and J. Zhang. A steganographic method for digital images with four-pixel differencing and modified lsb substitution. *J. Vis. Commun. Image R.*, 22(1):18, 2011.

[4] Marghny H. Mohamed, Naziha M. AL-Aidroos, and M. A. Bamatraf. Innovative multi-level secure steganographic scheme based on pixel value difference. *International Journal in Foundations of Computer Science & Technology (IJFCST)*, 2(6):1–13, 2012.

[5] S. Katzenbeisser and F.A.P. Petitcolas. *Information Hiding Techniques for Steganography and Digital Watermarking*. Artech house,Inc, 2000.

[6] Marghny H. Mohamed, Fadwa A., and Mohamed A. Bamatraf. Data hiding by lsb substitution using genetic optimal key-permutation. *International Arab Journal of e-Technology*, 2(1):11–17, 2011.

[7] Mohammed A.F. Al-Husainy. A new image steganography based on decimal-digits representation. *Computer and Information Science*, 4(6):38–47, 2011.

[8] Marghny H. Mohamed, Naziha M. AL-Aidroos, and Mohamed A. Bamatraf. A combined image steganography technique based on edge concept and dynamic lsb. *International Journal of Engineering Research & Technology (IJERT)*, 1(8), 2012.

[9] Naziha M. Al-Aidroos, Marghny H. Mohamed, and Mohamed A. Bamatraf. Hybrid cryptographic scheme for data communication. *International Conference on Advanced Computer Theory and Engineering (ICACTE 2009)*, 2009.

[10] William Stallings. *Cryptography and Network Security Principles and Practices*. Prentice Hall, fifth edition, 2011.

[11] Marghny H. Mohamed. Multi-service cryptographic scheme for secure data communication. *International Journal of Computer Science and Network Security (IJCSNS)*, 11(7):148–153, 2011.

[12] D. S. Abdul. Elminaam, H. M. Abdul Kader, and M. M. Hadhoud. Performance evaluation of symmetric encryption algorithms. *Communications of the IBIMA*, 8, 2009.

[13] A.P. Stakhov. The "golden" matrices and a new kind of cryptography. *Chaos, Solutions and Fractals*, 32:1138 – 1146, 2007.

[14] K.R. Sudha, A.Chandra S., and Prasad R. P V G D. Cryptography protection of digital signals using some recurrence relations. *IJCSNS International Journal of Computer Science and Network Security*, 7(5):203 – 207, 2007.

[15] Ayse N. On the hadamard product of golden matrices. *Int. J. Contemp. Math Sci.*, 2(11):537 – 544, 2007.

[16] Angel M. R. and Gerardo R. S. On the security of golden cryptography. *International Journal of network security*, 7(3):448 – 450, 2008.

[17] Shaligram P., Amber J., and Ramjeevan S. T. A novel approach for information security with automatic variable key using fibonacci q-matrix. *International Journal of Computer & Communication Technology (IJCCT)*, 3(3):54–57, 2012.

[18] A.P. Stakhov. Fibonacci matrices, a generalization of the cassini formula, and a new coding theory. *Chaos, Solitons and Fractals*, 30:56–66, 2006.

[19] T. Ando. Majorization relations for hadamard products. *Linear Algebra and its Applications*, 223 - 224:57 64, 1995.

[20] Ayse N. On the hadamard product of fibonacci q^n matrix and fibonacci q^{-n} matrix. *Int. J. Contemp. Math Sci.*, 1(16):753 – 761, 2006.

[21] Ben L. and Michael Z. An overview of complex hadamard cubes. *RHIT Undergrad. Math. J.*, 13(2):31 – 42, 2012.

[22] Ran T., Jun L., and Yue W. The multiple-parameter discrete fractional hadamard tranform. *Optics Communications*, 282(8):1531 – 1535, 2009.

[23] Adrian G. and S.K. Darwin. Theory and application of the fibonacci p-number. Technical report, Durham university, Communicating Mathematics III, April 2010.

[24] Stakhov OP. A generalization of fibonacci q-matrices. *Rep Nat haar wavelet*, 9:46–54, 1999.

[25] V.S.Bagad and I.A. Dhotre. *Networks And Information Security*. Wiley Publishing, Inc., 2009.

[26] Alexander Stanoyevitch. *Introduction to Cryptography with Mathematical Foundations and Computer Implementations*. Chapman and Hall/CRC, fifth edition, August 2010.

[27] Deborah R. *Statistics Essentials For Dummies*. Wiley Publishing, Inc., 2010.

[28] Yousef B. Mahdy Marghny H. Mohamed and Wafaa A. Shaban. Confidential algorithm for golden cryptography using haar wavelet. *(IJCSIS) International Journal of Computer Science and Information Security*, 12(8), 2014.

Marghny H. Mohamed received his Ph.D. degree in computer science from the University of Kyushu, Japan, in 2001, his M.Sc. and B.Sc. from Asyut university, Asyut, Egypt, in 1993 and 1988, respectively. He is currently a Professor in the Department of Computer Science, and for Vice Dean for Student affairs of Faculty of Computers and Information Systems, University of Asyut, Egypt. His research interests include data mining, text mining, information retrieval, web mining, machine learning, pattern recognition, neural networks, evolutionary computation, fuzzy systems, and information security. Dr.Marghny is a member of the Egyptian mathematical society and egyptian syndicate of scientific professions

Tammam Ali Tammam Muhammad is senior .net developer at Faculty of Computers and Information Systems, University of Asyut, Egypt. Received his Bachelor Science degree in computer science in 2004 at Assiut University, Faculty of Science, Dept. of Mathematics, Egypt and he is preparing the finale phase of his Master's degree in Cryptography, his research activities are currently focused on the information security.