International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

A Manipulated Cyclic Permutation Data Scrambling Approach for Data Security

OYINLOYE, Oghenerukevwe Elohor[1], Benson Ojedayo[2]

Ekiti State University, Ado-Ekiti, Ekiti State Nigeria

Abstract: ***Data sharing in every organization is a high-level priority asset. These are mostly kept electronically and exchanged via networks. The advances in technology, has made data vulnerable to manipulation and unreliable. Most techniques used to encrypt data have shown that they can be reconstructed using statistical approach with low time complexity. In this paper, a manipulated cyclic permutation system was developed for data encryption. The system performs its function by converting a plain text to cipher text and vice versa using the manipulated cyclic permutation method. The system was tested using 15 messages and showed to be 75% reliable and resisted the guessing attack proposed by users.***

Keyword: Cyclic permutation, data security, encryption, scrambling, matrix

1. Introduction

Most security techniques are application layer technology to guard transmitted information (ranging from speech, images to computer messages) against unwanted disclosure as Ill as to protect the data from unauthorized modification while in transit.
Rapid proliferation of computers and advances in information sharing has given rise to increased vulnerability with transmitted information. Data security is one of the most crucial challenges in digital world security. Privacy and integrity of data are demanded in every operations performed. When security of data is considered, it is mostly in the context of secure transfer of information over unreliable communication network [**2**].

In the ever-growing cyber world, millions of bytes of data are transferred everyday over the vulnerable interfaces; security of data becomes top priority. Secure transmission of confidential messages has become a common interest both in research and application. Attacks such as, eavesdropping, tampering have been melted on the integrity of transmitted data [**3**]. However, approaches have been proposed to secure data; which include variants of cryptography, steganography, access control is available.

Cryptography deals with the development of techniques for converting information between intelligible and unintelligible forms during information exchange [**4**].

Steganography is the art of hiding confidential information writing any file media to produce on amalgamated secret cover-media called stego-media in a way that prevents the disclosure of hidden information to unauthorized recipients [**5**]

2. Review of Data Encryption Approaches

Cryptography means the act and science of encrypting messages such that it is unintelligible to whoever is not authorized to have access to it . Cryptography relies on two basic components; an algorithm (a complex mathematical formula) and a key (string of bits) [8].

The two basic cryptographic techniques are
a) Symmetric and;
b) Asymmetric.

(a) Symmetric Cryptography
In secret key cryptography, the parties involved share the same key between themselves. The share is used to encrypt and decrypt data. This key is kept secret because if compromised, the security offered by the system will be adversely reduced. Examples of secret key system but not limited to DES [7];[9].

(b) Asymmetric Cryptography:
Public-key cryptography is a cryptographic approach which involves the use of asymmetric key algorithms instead of or in addition to symmetric key algorithms, it was first proposed in 1976 by Whitfield Diffie and Martin Hellman in order to solve the key management problem. Unlike symmetric key algorithms, it does not require a secure initial exchange of one or more secret keys to both sender and receiver. The asymmetric key algorithms are used to create a mathematically related key pair: a secret private key and a published public key, [10] likened public key cryptosystem, to a mathematical strong box with a special resettable combination lock that requires one type of combination to lock and another to open. Use of these keys allows protection of the authenticity of a message by creating a digital signature of a message using the private key, which can be verified using the public key [7]. It also allows protection of the confidentiality and integrity of a message, by public key encryption, encrypting the message using the public key, which can only be decrypted using the private key, but use too long phrases that most times have to be written down. Symmetric method has the problem of key management (symmetric key). Most public key infrastructure has problems of cost, registration process and need for internet [1].

3. An Optimum Modified bit plane splicing LSB Algorithm for Secret Data Hiding

The authors presented a method that uses steganography to hide data, in this method, the data is embedded in the LSB's of the pixel values, the pixel value are categorized into

different ranges depending on the range numbers of bit allocated to node the sensitive data. In this techniques, prime numbers are utilized not just the bit planes of the image but even the higher bit planes of the image thereby increasing the hiding capacity [6].

3.1 Design of the Manipulated Permutation Scramble System

The designed system is called a Manipulated Permutation Scramble System (MPSS) is an encryption and decryption tool used for securing data before and after transmission, it employed an abridged cyclic permutation method of encryption and decryption. Figure 1 shows the architectural structure of the MPSS

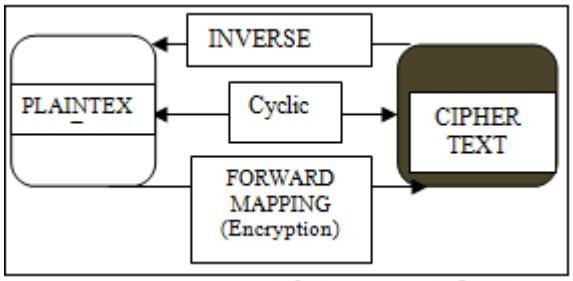

Figure 1: MPSS Architecture

3.2 Phases of the MPSS

The MPSS technique of encryption and decryption is a 3 module system namely:

1) The input module
2) The encryption module
3) The decryption module

Input Phase
This phase will interact with the user and determine if the login text provided is authorized, the operation of this phase is achieved by checking the input text given by the user if it correlate with the predefined inputs, a specified limit of trials is given and if the maximum number of trial is exceeded, access to input values is denied

Decision Phase
At this stage, details of how the transmitted message will before decrypted. The encrypted message will be shown after gaining access through the input phase, the receiver then performs cyclic permutation on the text based on the number of required time.

Encryption Phase
The encryption module utilizes the plaintext, the defined matrix and forward mapping.

The cyclic permutation is performed on the values starting from the determined row or column, the basic step is given below:

Step1
We formed the column and row matrix using cyclic permutation starting from column 5 for instance.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

E F G H I J K L M N O P Q R S T U V W X Y Z A B C D

Step 2
Compute the values of mapping making use of two step forward mapping for the encryption process. Assuming the data to be encrypted is
"MRS OYINLOYE IS MY SUPERVISOR" so that the cipher equivalent is given as "UZA WGVTWGM QA UG ACXMZDQAWZ"

Step 3
The plain text converted to cipher text using the key is then saved.

Decryption Phase
The decryption module also makes use of the plain text and the defined matrix, to decrypt the given text value, the receiver makes use of inverse (backward) mapping for the decryption process, the decryption process is an inverse of the encryption module the algorithm for the decryption phase.

Step 1
performing the cyclic permutation starting from Column 5

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

E F G H I J K L M N O P Q R S T U V W X Y Z A B C D

Step2: Decrypt the sent text value by performing backward mapping on each of the given text value of the encrypted form. For instance:

The plain text "MRS OYINLOYE IS MY SUPERVISOR". Figure 3 and 4 shows the encryption and decryption algorithm developed:

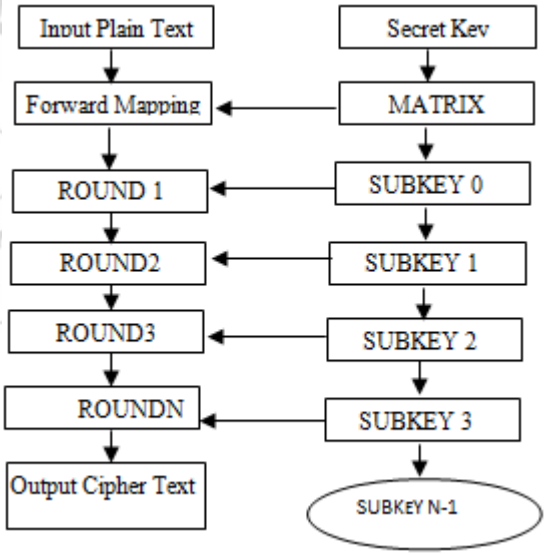

Figure 3: Encryption Algorithm

The cipher text "UZA WGVTWGM QA UG ACXMZDQAWZ" becomes

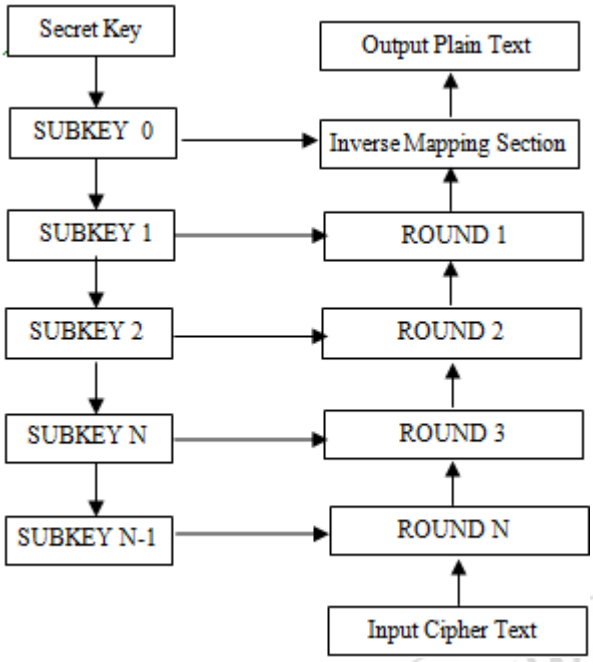

Figure 4: Decryption Algorithm

4. Result and Discussion

The system was tested using fifteen data sets, a snap shot of one result is shown in the figure 5 to 7.

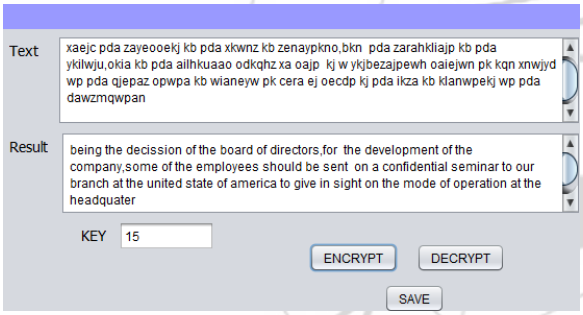

Figure 5: Data encryption

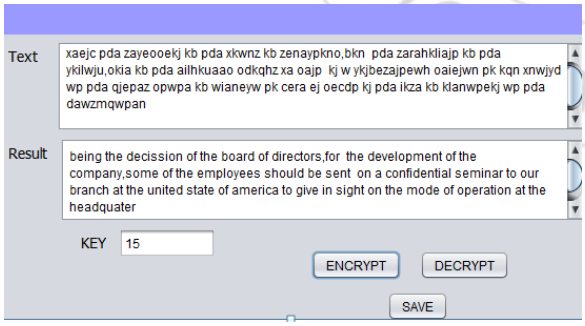

Figure 6: Data decryption

From the test, the system was evaluated to be 75% efficient in terms of data encryption.

5. Conclusion

The MPSS is a useful tool for preserving data at all levels of use. This approach may be susceptible to statistical based attacks but will require a relatively high data and time complexity, since the permutation does not follow the conventional cyclic permutation approach.

6. Recommendation

The MPSS is a data security approach from which more mathematical manipulations could be done.

7. Acknowledgement

We acknowledge the contributions of the following persons, Badmus Sakirat, Ogunyemi Adebola, Edokpa Daniel and Bello Olawale

References

[1] Oyinloye O.E, Alese B.K, Fasiku A.I, Akinbohun F (2011); Development of an Enhanced token using public key Infrastructure and Picture Password Algorithm for digital signature; International Journal of Computer Science and Information Security 9(10) pp:164-70 .

[2] Zhang D., SXU, Y. Wang, J.Zhang and Y.L. (2010): "a digital finger printing scheme of digital image" international conference on computational intelligence and software engineering). Vol 4, pp 13 – 15.

[3] Kreen, R., Stegno-graph and Stegno-analysis, http://www.kreennl/univ/cry/steg. accessed on 15th of May, 2015.

[4] Kaur K., k. Dhindsa, G. Singh, (2009): NurnErir to numeric encryption scheme: using 3KDEC algorithm, preceding of IEEE international conference on computing, pp 1501-1505.

[5] Gray C. Kessler, (2011) "an overview of stegangraphy for the computer forensics examiner". Practice Hall Publisher, pp 31 – 40.

[6] Naseem M., Ibrahim M.Huassain, M. Kamian Khan, Aisha Ajmal, (2011): "an optimum modified bit plane slicing LSB algorithm for secrete data hiding" international journal of computer applications, vol-25, Vol 12. Foundation of computer science new York, USA, pp 36-43.

[7] Mannivann, R-Surajannai, (2010): lightweight and secure data base encryption using TSFS algorithm, proceeding of the international conference on computing communication and network technologies, pp 1-7.

[8] Alese B.K. (2000), Vulnerability Analysis of Encryption/Decryption Techniques of Computer Network Security. MTech thesis Federal University of Technology, Akure.

[9] Iyare (2010). Developmet of a secure Information sharing system for E-policing (a case study of Ondo state police command) MTech thesis Federal University of Technology, Akure.

[10] Alese B.K. (2004), Design of Public Key Cryptosystem using Elliptic curve. PhD thesis Federal University of Technology, Akure.