A Novel Encryption Algorithm based on Auto Associative Neural Network and Soft Computing

Varsha Raj

Student, Dept. of Dual Degree Computer Applications, Christ Knowledge City, Kerala, India

---***---

Abstract - *Security is a major concern in our network communication. Cryptography is a field of computer science which satisfies our security requirements. The major duty of the cryptography is to conceal the confidential data from an insecure environment. It enables to send sensitive data securely over the communication network. The basic idea of the cryptography relies on the Encryption and Decryption techniques. In this paper a novel encryption algorithm is proposed which is based on the basic neural network concepts and soft computing*.

Key Words: **Cryptography, Encryption, Decryption, Neural Network, Soft Computing, Security, Algorithm.**

1. INTRODUCTION

Cryptography is an art of hiding the important, sensitive or confidential information from the unwanted usage. "Krypto" is the word from which the word, cryptography is evolved. It is basically a technique for the safe communication in the presence of an insecure third party. In general, the process of cryptography includes an encryption and decryption technique. Encryption is the process of applying a key to convert the plain text to the cipher text. Meanwhile, decryption is the process of using the same key to convert the cipher text back to its original form that is, the reverse procedure of the encryption. In this paper we use the neural network concept of soft computing in combination with encryption and mathematical techniques to send data securely on the communication network.

A neural network is a network of neurons. An artificial neural network is composed of artificial neurons/nodes. The connections of the nodes are modeled as weights. All inputs are modified by a weight. Artificial neural network may be used for predictive modeling, adaptive control and for training datasets. Auto Association network is a type of memory that enables one to retrieve a piece of data from only a tiny sample of itself. An auto associative neural network is used for the purpose of recognizing a given input pattern as known or unknown. An input pattern is categorized as known if and only if the network produces the output exactly same as the input for that pattern. So the testing algorithm is used to test the network by checking whether the network is recognizing the patterns or not. The concept of using neural networks in the field of cryptography is a novel approach and different from the authentic encryption techniques.

2. EXISTING SYSTEM

The authors (D.Suneetha, D.Rathna Kishore, G.S.Pradeep [1]) together proposed security model improves the confidentiality level of data with the help of Artificial Neural Networks which also improves the security of data over cloud environment. The Dynamic fragments model stores highly sensitive fragments in the corresponding data center over the cloud and also use encryption algorithm in combination with cascading feed forward network to obtain relevant cipher text.

Cryptography is a science of hiding the important data in the insecure network and it involves encryption to convert plain text into cipher text and decryption to convert the cipher text into the plain text. Cryptographic model is of basically two types one is symmetric model and asymmetric model. The existing system has different cryptographic algorithms that we are using currently:

2.1 Public Key Cryptography

Public key Cryptography is a cryptographic system where asymmetric cryptography model is used. Authors (Dahu Wang, Heyuan Bai, [2]) states that" There are a minimum of two keys during a public-key cryptosystem or non-symmetric cryptosystem: the public key and the secret key, or several of them. For the secret key to remain a secret it must be computationally very challenging to calculate the secret key starting from the public key. The public key can be left in a "place" where anyone who wants to can take it and use it to send encrypted messages to the owner of the secret key". In this for encryption of plain text public key is used and public key is known by all the users in the network that is why it is called as shared key. Decryption of cipher text in public key cryptography is done using private key only which means if receiver is having the respective private key then only the receiver can decrypt the message. Private Key is a secret key which is only known to the respective users and is hidden from others in the network.

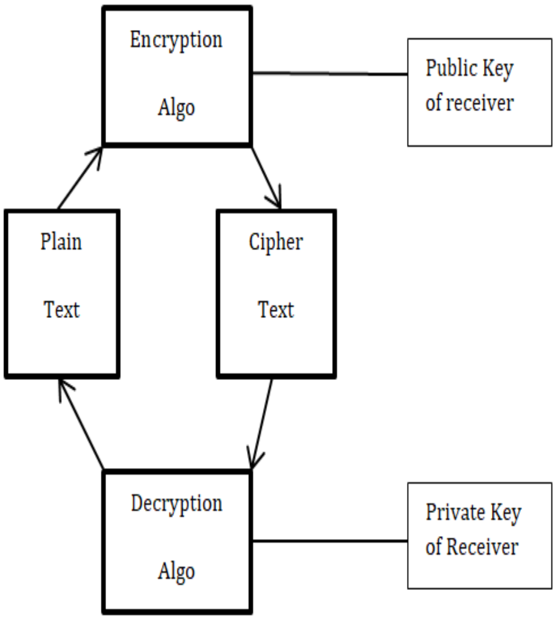


Fig 1: Public Key Cryptography

2.2 Private Key Cryptography

Private Key Cryptography is a cryptography system where symmetric cryptography model is used. In this for encryption of plain text secret key is used which is private key and for decryption of cipher text also here same secret key is used. The Authors (Sourabh Chandra, Smita Paira [3]) states that "Symmetric key cryptography is also called Secret-key or shared key cryptography. In this type of mechanism, the sender and receiver shares a common key for both encryption and decryption. The method follows self-certification method i.e. the key is self-certified. The key needs to be shared through secret communication. If it is compromised then the encrypted message can be easily decrypted by the attacker. This type of cryptographic technique is required because it provides faster service without using many resources. Various algorithms have been developed so far to describe symmetric key cryptography. These are AES, DES, 3DES, Blowfish". As here in both the cases of encryption and decryption similar key is used so it is called shared secret key. Shared key used here is unique key for a session and is only disclosed to the sender and the receiver.

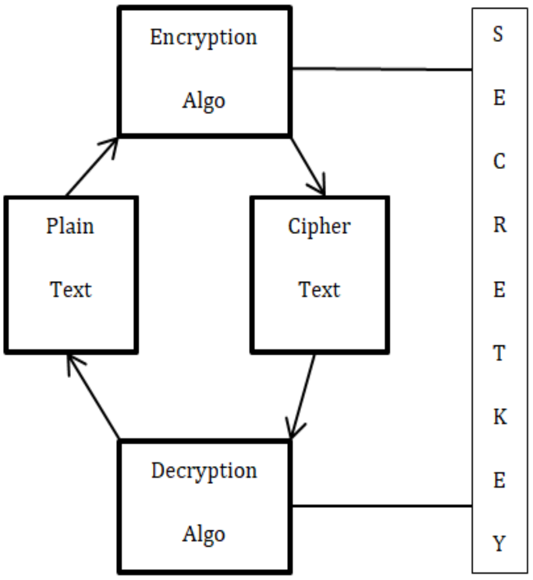


Fig 2: Private Key Cryptography

2.3 Cryptographic Hash Function (CHF):

A cryptographic hash function (CHF) may be a hash function that's suitable for use in cryptography A hash function is the mathematical function that converts a numerical input value into another compressed input value. It accepts a variable length block of data and produces a fixed size hash value. Cryptographic hash functions are a basic tool of recent cryptography.

3. METHODOLOGY

In this paper a novel encryption algorithm is proposed which is based on the basic neural network concepts and soft computing. Encryption and decryption on an algorithm is done by either a private key or a public key as we discussed earlier.

We use a private key to be known by the sender and the receiver. We use this key for both the encryption and decryption. The key is a matrix. It will be a matrix of size k*j, where k=2 and j is the even numbers 4, 6, 8 etc. Then even columns (0, 2, 4, 6,...) will be filled with zeros, whereas the other columns will be filled with the either 1s or -1s. The key will be known to both the sender and the receiver[4]. We use binary values to be treated by the algorithm.

3.1 Encryption Algorithm

- ➢ Convert the plain text to the binary digits
- ➢ We have the key matrix as K
- ➢ Replace the even columns of K matrix with the Plain text. It will be weight matrix, W.

- Multiply the weight matrix, W with the key Matrix K forms the matrix J.
- Multiply the J matrix with the key matrix forms a Matrix C.
- The matrix C will be our Cipher text.

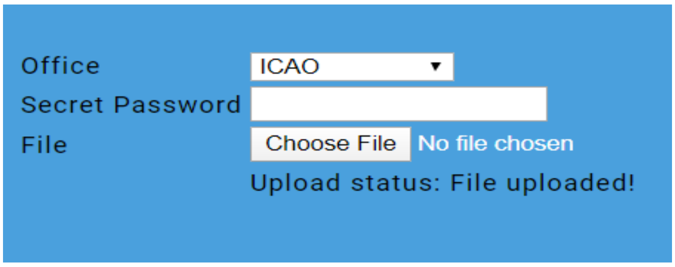
3.2 Decryption Algorithm

- Multiply the Cipher text matrix C with the inverse of key matrix L forms a matrix S.
- Multiply S with the Matrix L
- Even columns will have the plain text.
- Apply the Activation function
- Convert the plain text back to strings/words

4. FUTURE WORK

The algorithm is beneficial for the security terms like other cryptographic algorithms do. It can be applied to different areas like Defense, Aviation, Banking, Medical field etc. This algorithm can be used for the password authentication. It can be used for secret communication in any fields like Aviation, Defense or any other application areas which requires the sharing of highly confidential or sensitive information.

The Figure below shows an application area which uses this algorithm for secret communication for the aviation sector.



Office ICAO
Secret Password
File Choose File No file chosen
Upload status: File uploaded!

Fig 3: Application Area

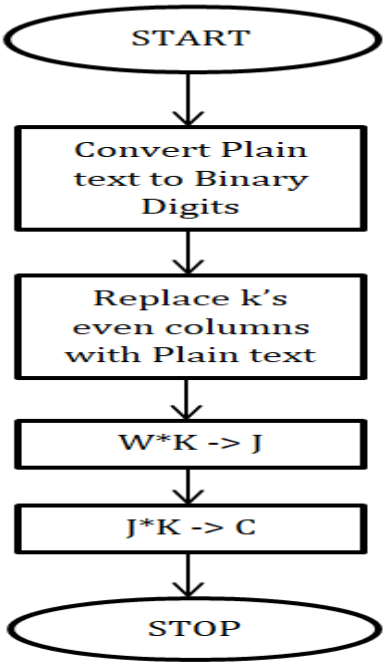

START
Convert Plain text to Binary Digits
Replace k's even columns with Plain text
W*K -> J
J*K -> C
STOP

Fig 4: Flow Chart of Encryption Algorithm

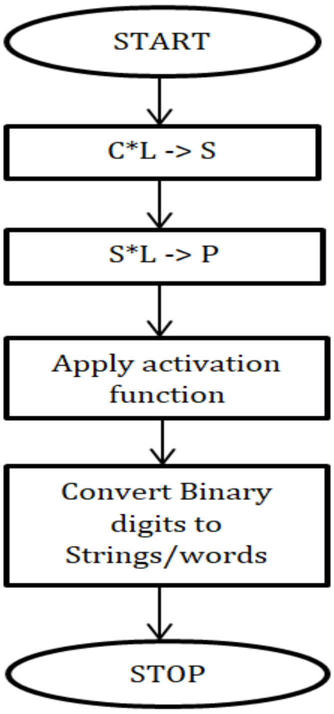

START
C*L -> S
S*L -> P
Apply activation function
Convert Binary digits to Strings/words
STOP

Fig 5: Flow Chart of Decryption Algorithm

5. CONCLUSION

In this paper a novel encryption algorithm is proposed which is based on the basic neural network concepts and soft computing. The combination of the cryptographic algorithms with the neural networks is growing in an expeditious manner. In this proposed algorithm, the encrypted form will be totally dissociated from the antecedent. The algorithm can carry out in areas like Defence, Aviation, Banking in an effortless manner and with quick encryption and decryption pace.

ACKNOWLEDGEMENT

I would like to extend my heartfelt thanks to our HoD, Er.Geethu Krishna Kartha, Department Of Dual Degree Master of Computer Applications for the helps extended to me throughout my course of study. I am deeply grateful to my guide Ms Elsa Sabu, Assistant Professor, Department of Dual Degree Master Of Computer Applications for the valuable guidance. My sincere gratitude towards Ms Aimy Susan Thomas, Assistant Professor for the encouragement and support. I'm deeply indebted towards Er Saranya shaji, Assistant. Professor, for the valuable advices.

REFERENCES

[1] D.Suneetha, D.Rathna Kishore, G.S.Pradeep, "Data Security Model using Artificial Neural Network and Database Fragmentation in Cloud Environment" IJRTE, vol.08, Issue 02 July 2019.

[2] Dahu Wang, Heyuan Bai, "A Public Key Cryptography and a Entity Authentication Scheme based on Improved Hyperbolic Function"IEEE, 2008.

[3] Sourabh Chandra, Smita Paira, "A Comparative Survey of Symmetric and Assymmetric Cryptography" IEEE, 2014, International Conference on Electronics, Communication and Computational Engineering (ICECCE).

[4] Pavi Saraswat, Kanika Gharg, "Encryption Algorithm based on Neural Network," IEEE 2019