Adaptive Neuro- Fuzzy inference Based Pattern Recognition Studies On handwritten Character Images

Kamble Ajay Babruwahan

1. Introduction

The necessity of information security within an organization has undergone major changes in the past and present times. In the earlier times physical means is used to provide security to data. With the advent of computers in every field, the need for software tools for protecting files and other information stored on the computer became important. The important tool designed to protect data and thwart illegal users is computer security.

With the introduction and in communications, one or more change that affected security is the introduction or distributed systems which requires carrying of data between terminal users and set of computers. Network security measures are needed to protect data during their transmission. The mechanisms used to meet requirements like authentication and confidentiality are observed to be quit complex.

Security mechanisms usually involve more than a particular algorithm or protocol for encryption & decryption purpose and as well as for generation of sub keys to be mapped to plain text to generate ciphere text. It means that participants be in profession of some secret information (Key), which can be used for protecting from unauthorized use.

rs. Thus a model has to be developed within which security services and mechanism can be viewed.

To identify and support the security services of an organization at its effective level, the manager needs a systematic way. One approach is to consider three aspects of information security attack, Security mechanism and Security services. Security attack identifies different modes by which intruder tries to get unauthorized information and the services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

As the important of information systems is ever growing in all most all fields, electronic information takes on many of the roles, earlier they being done on papers. Few information integrity functions that the security mechanism has to support are security and confidentiality of the data to be transmitted and authentication of users.

There is no single mechanism that will provide all the services specified. But we can identify a very important mechanism that supports all form of information integrity are cryptographic technic. Encryption of information is the most common means of providing security. A model for encryption can be represented by the following Figure 1.1

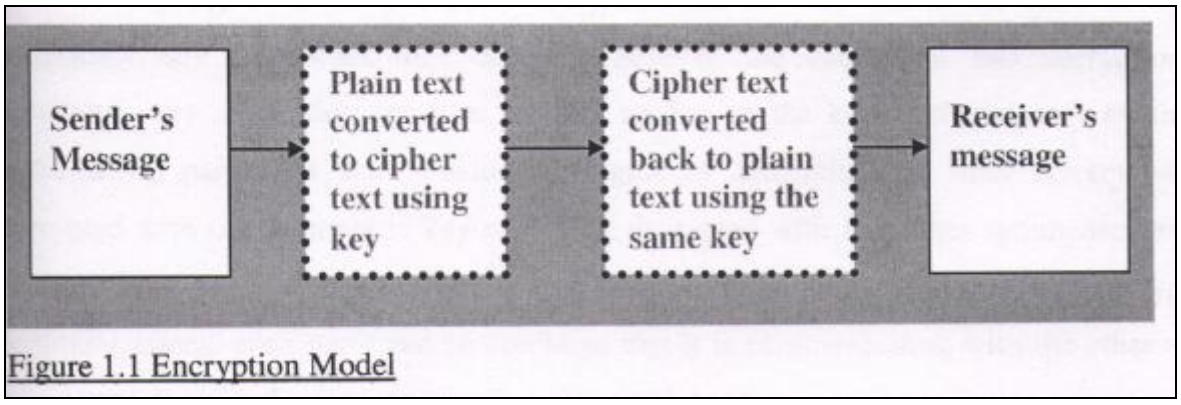


Figure 1.1 Encryption Model

This general model shows that there are four basic tasks in designing a particular security service.

1. Designing and algorithm for performing encryption & decryption process.
2. Generating the secret information with the help of algorithm of step 1.
3. Identifying methods for the distribution and sharing of secret information.

4. Identifying rules to be used by both the participating parties to make it secured.

A crypto system is an algorithm, plus all possible plain texts, cipher texts and keys. There are two general types of key based algorithms symmetric and public key. With most symmetric algorithms, the same key is used for both encryption and decryption as shown in Fig 1.2

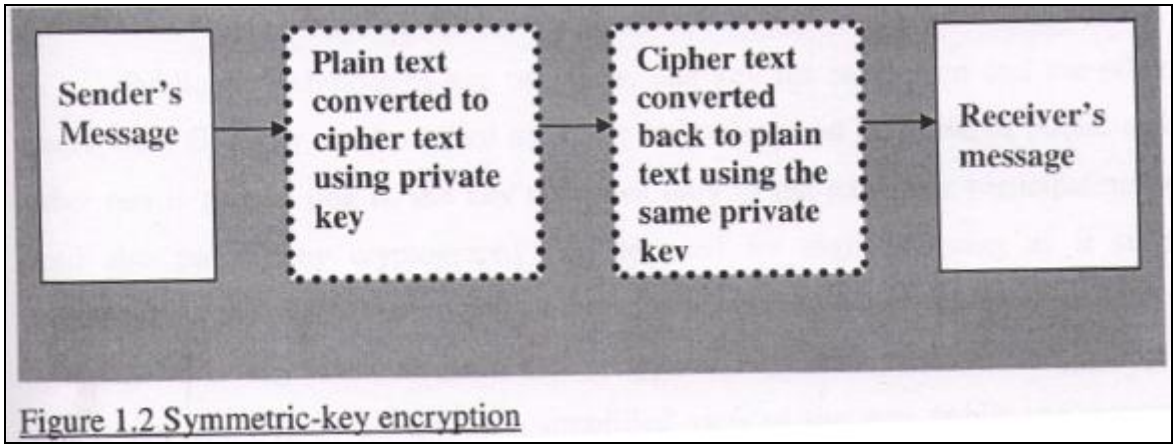


Figure 1.2 Symmetric-key encryption

2.1 Symmetric Encryption Schemes

Decryption key and vice versa. With most symmetric algorithms, the same key is used for both encryption and decryption as shown in Fig 1.1. Implementations of symmetric key can be highly efficient, so that users do not experience any significant time delay as a result of the encryption and decryption. Symmetric –Key encryption also provides a degree of authentication, since information encrypted with one symmetric key cannot be decrypted with any other symmetric key. Thus, as long as the symmetric key is kept secret by the two parties using into encrypt communications, each party can be sure that it is communicating with the other as long as the decrypted message continue to make sense.

Encryption functions normally take a fixed-size input to a fixed-size output, so encryption of longer units of data must be done in one of two ways; either a block is encryption of longer units of data must be done in one of two ways; either a block is encrypted at a time and the blocks are somehow joined together to make the cipher text, or a longer key is generated from a shorter once and XOR'd against the plaintext to make the cipher text. Schemes of the former type are called block ciphers, and schemes of the later type are called stream ciphers.

2.1.1 Block Ciphers

Block ciphers take as input the key and a block, often the same size as the key. Further the first block is often augmented by a block called the initialization vector, which can add some randomness to the encryption.

2.1.1.1 Block Ciphers

The most widely used encryption scheme is based on Data Encryption Standard (DES). There are two inputs to the encryption function, the plain text to be encrypted and the key. The plain text must be 64 bits in length and key is of 56 bits, first the 64 bits of plain text passes through an initial permutation that rearranges the bits. This is followed by 16 rounds of same functions, which involves permutation & substitution functions. After 16 rounds of operation, the pre output is swapped at 32 bits positions which are passed through final permutation to get 64 bit cipher text.

Initially the key is passed through a permutation function. Then for each of the 16 rounds, a sub key is generated by a combination of left circular shaft and permutation. At each round of operation, the plain text is divided to two 32 bit halves, and the following operations are executed on 32 bit right halve of plain text. First it is expanded to bits using

an expansion table, then X-ORed with key, and then processed in substation tables to generate 32 bit plain text will from left 32 bit pre cipher text of first round.

Decryption uses the same algorithms as encryption, expect that the application of sub keys is reversed. A desirable property of any encryption algorithm is that a small change in either plain text or the key should procedure a significant change in cipher text. This effect is known as available effect which is very strong in DES algorithm.

3. Methodology of the Proposed Work

The following sequence of steps identifiers the methodology adopted in this work.

1. Definition of the problem.
2. Algorithms for generation of sub keys
3. An algorithm 1 which multiplies ternary vector a random matrix key to generate a sequence. Dividing the sequence generated in algorithm 1 into basins based on equality of values. Mapping of the sequence or basins to the plain text to generate cipher text. This mapping develops 3models which are discussed in detail as subunits. The developed algorithm is trained to find an optimal key.
4. An algorithm 2 which considers a key, a time stamp and an Initialization vector to generate sub keys which are mapped to plan text to generate cipher text.
5. Training of the developed algorithms with different keys.
6. Adopting a suitable mechanism to identify any garbled key while transmission from the Key distribution Centre.
7. Comparative study of developed algorithms in terms of computing power, their Complexity in terms construction & strength, Avalanche effect & security analysis.
8. Comparative study of the algorithms with standard models like DES & RC4.
9. Summary & Conclusion of the work.

A New Substitution Block Cipher

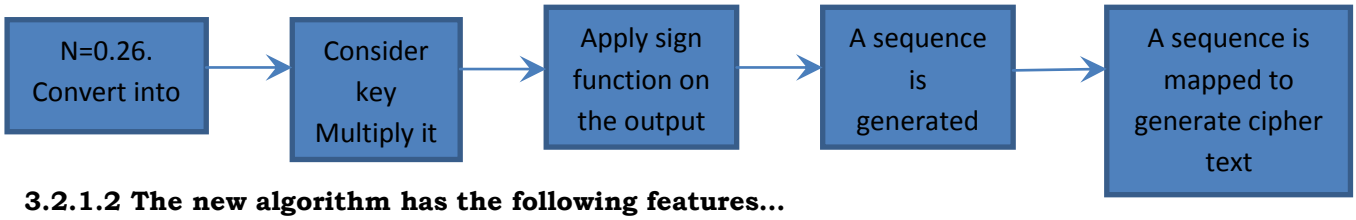
Model 1

3.2.1 A New Substitution cipher for data security.

The algorithm that is going to be discussed in the work will generate a Sequence. The algorithm

M considers a matrix key and executes a sequence of steps which generates the sequence. Each block of plain text is replaced by summation of alphanumerical value of the plain text and sequence generated to from cipher text. Thus the cipher text obtained becomes computationally infeasible to break without knowing the key.

3.2.1.1 Model 1: A new Substitution cipher for data security.



3.2.1.2 The new algorithm has the following features...

1. A set of poly alphabetic substitution rule is used.
2. A new block cipher is developed.
3. A random matrix is being used as key.
4. Generated sequence being used as sub key.
5. Coding method.

The steps that are involved in proposed algorithm.

1. The decimal values and letters of the plain text are given numerical values

3.2.1.8 Security Analysis

The model uses a sign function on the product of ternary vector and a matrix key to generate the sequence. The sign function converts all positive values to 1, negative values to -1, and zero with 0. This sequence is substituted for plain text to generate cipher text. Thus it is impossible to generate the matrix key from the known plain text and cipher texts. Thus this model is free from differential crypto analysis.

But this model uses a simple substitution technique to generate cipher text; it is somewhat susceptible to linear crypto analysis. The key cannot be gained and not a whole of information can be gained, but part of information may be gained in this model. This algorithm is completely free from cipher text only, type of attack, by the other attacks, the key may not be retrieved but part of plain text may be retrieved.

3.2.1.9 Conclusion.

In this work a ternary system with a 3 digit number is used. So the sub key generated is a 3^3 i.e. 27 digit number. By considering a ternary vector with a four digit number or five digit number, the length of the sub key can be increased by 3^4, 3^5 which increase the length of sub key generated. Similarly by considering n –ary vector the length of the sub key generated can still be increased Thus by increasing the length of the sub key security of cipher system can be increased still further.

Thus we can see that by changing the key values slightly, by changing the time stamp the model is generating variable and distinct values which provides sufficient strength to the algorithm. The algorithm can be made still stronger by varying the nonce value which generates variable sub key values.

4.2 Role of Statistical tests on values generated by the algorithms under study.

In the given study, two algorithms are discussed. Both the algorithm executes a series of steps and generates a sequence. This sequence is being used as sub key to be mapped to plain text to generate cipher text. The strength of encryption & Decryption process depends on the strength of sequence generated. In this part of work some statistical tests like uniformity tests, Universal tests & repetition tests ae tried on the sequence generated to test the strength of it.

Uniform test tries to study the uniformity of a sequence generated. Form the sequence generated the first two consecutive points re considered as coordinates of a graph. For example if a,b,c,d… n are the values of sequence generated, then the coordinates of graph are (a,b), (c,d)….. (n-1,n). if they are dependent they will form into lines or they will form into plane, in this study, different cases are tried for both the algorithm to study the non-uniformity distribution of values in sequence.

Universal tests: It tries to see whether the data can be compressed. Since in the given sequence, the repetition of value is minimum, we can say that the developed sequences are relatively free from this test.

Repetition test: This test studies that each character of the sequence is not identical to the earlier character. In the sequence generated by the first algorithm, the values are random and unique in nature; the probability that the values get repeated is 1/27. In the second algorithm even through some values of the sequence are repeated the distribution of values is not uniform and random in nature which does not give any insight about the pattern of the sequence. Thus we can say that the sequence generated by both the algorithms is relatively free from Uniformity test, Universal test & repetition tests.

The analysis is being done on sequence generated by both the algorithms which are represented as case studies in the earlier part of the work. The analysis is being represented as graphs for both algorithms.

Summary and Conclusions

This study represents the importance of Encryption of data for storage and transmission. The significance of encrypted data can be identified in light of the mushrooming

applications and globalization of communication. The advantages of encrypting data manifest themselves in the form of security & confidentiality in real time applications. Encryption of data is particular significance in applications like E- mail, E- Commerce, E-Cash were highly vulnerable communication lies is accessed for transmission of highly volatile data.

The study traces the development of various encryption models in a real time environment in all their breath taking diversity and breakthrough in chapter 2. The significance of the advances and adaptabilities is measured interms of their diversity of applications in myriad ways that we feel in our daily lives.

The chapter 3 identifies the methodology used in the developed work. It is classified as two algorithms. The first algorithm generates a sequence followed by model to generates sub keys and mapping of sequence or the sub keys on plain text to generate cipher text. The second algorithm considers a key, a time stamp & a nonce value to generate sub keys which mapped on plain text to generate cipher text.

Chapter 3.2.1 builds a new block cipher algorithm considers a matrix key and executes a sequence of steps which generates a sequence. The block of plain text which is of equal length to the length of sequence generated is considered. Each Character in this plain text is replaced by a corresponding numerical value added by a value from the generated sequence. Thus the cipher text obtained becomes difficult to break without knowing the key. The strength of generated model is studied in terms of computing power, avalanche effect, and complexity of the model in terms of construction & strength. A crypto analysis of the model is also identified to study the security of the developed model.

Chapter 3.2.2 builds a new variable length key block cipher algorithm. The algorithm considers a matrix key and executes a sequence of steps which generates a sequence. Based on the similarity of values this sequence is being divided into basins. The basins with minimum values will be eliminated. Remaining each basin represent one block of data. Depending on starting input plain text character, corresponding basin is considered as a key. The procedure is repeated for certain plain text depending on chosen value, thus the cipher text obtained becomes very difficult to be broken without knowing the key. The strength of generated model is studied in terms of computing power. Avalanche effect and complexity of the model in terms of its construction & strength. A crypto analysis of model is also identified to study the security of the developed model.

Chapter 3.2.3 builds a new stream probabilistic cipher algorithm. The algorithm considers a matrix key and executes a sequence of steps which generates a sequence. Based on the similarity of values this sequence is being divided into basins each basin represents one character. Each character in the plain text is replaced by a set of basins based on chosen base value. Each basin value is replaced by random values from basins to generate the cipher text. Thus multiple cipher text will be developed for one plain text. Any one cipher text can be used for data transmission. Thus the cipher text obtained becomes computational infeasible to be broken without knowing the key. The strength

References

1. Amjay Kumar, Ajay Kumar: Development of New Cryptographic Construction using Palm print Based Fuzzyvoult, EURASIP Journal on Adv. In signal Processing Vol21, pp 234-238, 2009

2. Baocang Wang, Qianhong Wu, Yupu Hu: A Knapsack Based Probabilistic Encryption scheme, On line March 2007 www. Citeseer. Ist.psu.edu

3. Bluekrypt 2009: Cryptographic Key length Recommendation http:// www. Keylength.com

4. Blum L., Blum M, Shub M. : A simple unpredictable psedo random member generator, SIAM J. Compute , 1986, 15 (2), pp 364-383

5. Brics: Universilly comparable notions of key exchange and secure channels, lecture notes in Computer Science, Springer Berlin, March 2004.

6. Sage Math.Washington.edu/home/jetechv/Public.html/docs/jetchv-talk.ppt-broadcast encryption schemes.

7. Brassard G : modern Cryptology, a tutorial lecture Notes on computer science, (325), (Spring-Verlas)

8. Bruce Scheneiner : applied Cryptography (john Wiley & Sons (ASIA) Pvt. Ltd.

9. Carlone Fontaine & Fabine Galand: A survey of Homomorphic Encryption for non specialists EURASIP Journal, VOl 07 Article 10.

10. Donavan G Govan, Nathen Lewis: using Trust for Key Didtribution & Route Selection in wireless sensor Networks, International Conference on Network Operations & management, IEEE Symposium 2008, PP 787-790.

11. Dorothy E Denning Et al. Time Stamps in Key Distribution protocol Communication of ACM, Vol 24 Issue 8 Aug 1981 pp 533-536

12. E.C. Park, I F Blake. Reducing Communication overhead of Key Distribution Schems for Wireless Sensor Networks: Computer Communications & Networks ICCCN 2007, pp 1345-1350

13. Georg H Fuchsbauer : An Introduction to Probabilistic Encryptin Osjecki