Sahel Journal of Life Sciences FUDMA (SAJOLS)
September 2025 Vol. 3(3): 71-76
ISSN: 3027-0456 (Print)
ISSN: 1595-5915 (Online)
DOI: *https://doi.org/10.33003/sajols-2025-0303-10*

Research Article

Modified Amino Acid Encryption Method Using Bi-directional Associative Memory Neural Network for Key Generation

[*]A. Abdulkadir[1], M. Bello[2] and S. Ahmad[3]

[1]Department of Computer Education, Isa Kaita College of Education, P.M.B 5007, Dutsin-Ma, Katsina State, Nigeria
[2]Department of Computer Education, Isa Kaita College of Education, P.M.B 5007, Dutsin-Ma, Katsina State, Nigeria
[3]Department of Computer Science, School of Technology Kano State Polytechnic, Nigeria
***Corresponding Author's email*: aakado123@gmail.com**

ABSTRACT

The paper proposed a modified amino acid-based encryption model that uses a bi-directional associative neural network for key generation, used for encryption and decryption. The proposed model survived against several attacks, such as plaintext, known plaintext, and cryptanalysis, and a comparative analysis was carried out based on encryption and decryption time between the original algorithm and the modified model, and the result shows that both models have the same encryption and decryption time.

Keywords: Amino acid; Cryptosystem; DNA; Decryption; Encryption

Citation: Abdulkadir, A., Bello, M., & Ahmad, S. (2025). Modified Amino Acid Encryption Method Using Bi-directional Associative Memory Neural Network for Key Generation. *Sahel Journal of Life Sciences FUDMA*, 3(3): 71-76 DOI: *https://doi.org/10.33003/sajols-2025-0303-10*

INTRODUCTION

Introduction Internet and wireless networks offer ubiquitous channels to deliver and exchange data. Some models, such as cryptography, are used to improve the security of data transfer. Cryptography keeps data secured by ensuring that it is not understandable to unauthorized persons. The method of cryptography is the process of converting ordinary information (plaintext) into unintelligible cipher text (i.e., cipher text). More information is sent to the receiver and divided into components of the hidden message or picture that makes access to all pictures at once hard for the transgressors (Mirjalili *et al*., 2020). This increases the safety at greater stage that is much required. This makes detecting and decoding a document very difficult for the intruders. Cryptography can be classified as a symmetric or asymmetric key. Symmetrical core involves methods such as Data Encryption Standard (DES), Advanced Encryption Standard (AES) and asymmetrical include Diffie Hellman, Rivest–Shamir–Adleman (RSA) and other such methods (Mirjalili *et al*., 2020). The cipher block duration is inflexible for example in DES, AES algorithms. Only one block of cipher can be encoded by Random Block Length Based cryptosystem through Multiple Cascaded (RBCMPCC). Any intermediate block chosen as the encrypted block within the RPSP algorithm during its phase serves as the hidden key. However, as a result, decryption keys must be very difficult to access and use by the intruder, so that only the intended recipients can read the encrypted messages (Praneetha, 2020). Some potential model for key generation is the use of bi-directional associative neural network but some implementation uses Genetic algorithm (GA) (Praneetha, 2020). The encryption system in modified amino acid cipher uses machine learning for key generation and DNA-based encryption to improve security. DNA-based encryption is an emerging approach for information security because of its capabilities. In biology, DNA is the master molecule whose structure encodes all the

information needed to create and direct the chemical machinery of life. In 1953, the structure of DNA was correctly predicted by Watson and Crick. They predicted that DNA molecules consist of two long polynucleotide chains. Each of these chains is known as a DNA chain, or a DNA strand, which is made up of simple subunits, called nucleotides. Each nucleotide consists of a sugar-phosphate molecule with a nitrogen-containing side group, or base. The bases are of four types—adenine, guanine, cytosine, and thymine—corresponding to four distinct nucleotides, labeled A, G, C, and T (Bajaj and Sangwan,2019). In the proposed model, bi-directional associative memory neural network is used to generate a random key for encryption and decryption. The generated key is used to encrypt data using DNA encryption.

Organization of Paper

The paper is organized as follows: first we discuss a review of related work, next we explain the proposed model, then we report the simulation results and performance analysis, and finally we discuss the conclusions.

Classical play fair cipher Algorithm and working procedure

A play fair cipher is another form of a poly alphabetic cipher used by the British army during world war I. the secret key of in his cipher used for encryption is made of 25 alphabet letters arranged in a 5 by 5 matrix (letter I and J are considered the same when encryption) different arrangement of the letter in the matrix can create many different secret key .One of possible arrangement is Before encryptions, if the two letters in a pair are the same, a bogus letters is inserted to separate them. After inserting bogus letters ,if the number of characters in the plaintext is odd, one extra bogus character is added the end to make the number of characters even.

Rules use for encryption

This shows how traditional play fair cipher work which shows the end procedure used in encrypting protein or converted protein text to cipher text protein.

1. If the two leers in a pair are located in the same row of the secret key, the corresponding encryption characters for each letter is the next letter to the next letter to the right in the same row (with wrapping to the beginning of the row if the plaintext letter is the last character in the row)
2. If the two letters in a pair are located in the same column of the secret key, the corresponding encrypted character for each letter is the letter beneath I in the same column (with wrapping to the beginning of the column if the plaintext letter is the last character in the column)
3. If the two letters in a pair are no in the same row or column of the secret, the corresponding encrypted character for each leer is a letter the letter beneath I in the same column (with wrapping to the beginning of the column

REVIEW OF LITERATURE

The authors (Ahmed *et al*., 2022) proposed a bio-inspired cryptographic system using DNA system. The proposed method consists of three phases. The proposed crypto system is compared with traditional cryptographic that has Genetic algorithm scheme with NW techniques which had resulted in 55 and 67% increased processing time for encryption process and decryption process. The proposed cryptosystem uses both machine learning and biological approaches and is capable of providing security as well as efficient storage to data, which makes it possible to encrypt and decrypt even large amounts of data. It is proved that the key generation with BAMNN could originally demonstrate expensive as regards to memory for less bytes, it is obvious. But with more bytes, BAMNN's memory generation is faster even when more keys have been produced owing to its memory usage. This is due to its memory occupancy even with a greater number of keys being generated. The author (Basu *et al*., 2019) proposed bio –inspired crypto system that uses both machine learning and biological approaches capable of providing security as well as efficient storage of data. The crypto system entails generating a random key using a bi-directional associative memory neural network (BAMNN). The bi-directional associative memory neural network (BAMNN) is trained to generate the keys for every corresponding block input. The first block is generated randomly and further block are generated using the BAMNN process. The encryption process of this Cipher comprises of stages for converting the plaintext to binary form then generated 16 bits binary to DNA code, converting again the DNA generated code to the mrA form and finally from mrA to cipher text containing protein based. In this proposed system, Memory space are saves even in case of larger sizes of data, this means that the memory storage is significantly reduced with increased in the size of input data. Based on comparison of the proposed scheme using encryption and decryption time, the scheme does not give sufficient performance

compared to the scheme proposed in Zhanga and Liub (2017) and the performance is relatively better than the scheme proposed by Asghar *et al*. (2020). Also, the proposed scheme is proven by the authors' to be secured to some types of attack such as cipher attack, brute force attack cipher text attacks and etc. Also, an OTP encryption scheme which uses DNA-based random key generation was proposed by Zhanga and Liub (2017), which was proved to be unbreakable in theory but it's difficult to realize in practical application. Analysis has demonstrated that the proposed DNA-based random key generation and management solutions are marked by high security and usability, the work has addressed the difficulty of generating such pure random sequences as well as the management of these secure keys (to transmit and store them securely).

MODEL PRESENTATION

The proposed crypto system model has three phases: the first phase is the key generation in which a bi-directional associative memory neural network (BAMNN) is used to generate random key. while in the second phase the message data is converted to amino acid throw mutable operation and under goes series of transformation i.e. transcription and translation. In the third phase the key generated from a bi-directional associative memory neural network (BAMNN) used to encrypt amino acid data using play fair cipher.

Second Phase:

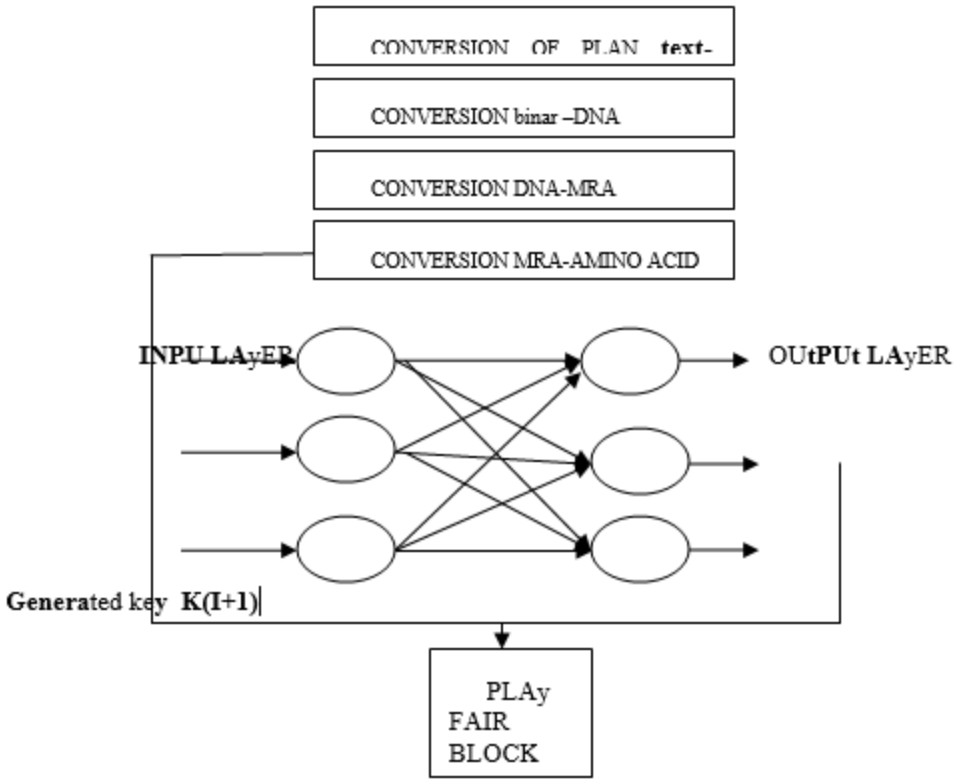
Data Preparation The plain data is converted to 8-bit binary format, and then converted to a DNA Nitrogen Base sequence. Then the DNA Nitrogen Base sequence obtained from the first step is converted to an RNA Nitrogen Base which was converted to an amino acid according to RNA to Amino Acid and the Ambiguity number called Protein Key (PK) is extracted.

Third Phase:

Data Encryption Using Amino Acid Based Playfair cipher is used which is the traditional play fair cipher, in which diagrams in plaintext are treated as single units and these units are translated into cipher text diagrams. Play fair encrypts pairs of letters. The traditional Play fair algorithm is based on a 5×5 matrix of letters constructed using a key in the model, the key generated from a bi-directional associative memory neural network (BAMNN) is taken as cipher key, and the alphabet is the modified amino acid alphabet. The data preparation phase and the encryption phase are depicted in the table given below. Also, a simple example of the proposed algorithm or system is shown in Fig. 6. The algorithm steps of the encryption process are shown as follows.

Key generation phase

A bi-directional associative memory neural network (BAMNN) is trained to generate the key for every corresponding block of input. The first block is generated randomly and further blocks are generated using the BAMNN process. The architecture of the key generation algorithm in the proposed system is depicted in figure above. The key generation process is mainly carried out using neural network with the proper of bi-directional associative memory. The weigh matrix W is used to represent the weight of the neural network. In this case, it's a 8 by 8 matrix of 64 weigh. These weights are trained using random binary noise. The final matrix is used for the purpose of key generation. Since the neural network uses both its input and outputs as key, the number of input and output neuron is required to be equal.



Pseudo code of modified encryption algorithm with BAMNN Keys:

Algorithm 1: Algorithm of encryption process Input, Message (M), Generated key using neural network: Protein Cypher (PC), Protein Key (PK)

1. Step 1: Input Message (M), Genetic KEY (K1)
2. Step 2: Convert Message (M) to 8-bit binary format (biM)
3. Step 3: Convert binary Message (bim M) to DNA Nitrogen Base (MDNA)
4. Step 4: Convert Message DNA Nitrogen Base (MDNA) to RNA Nitrogen Base (MRN)
5. Step 5: Convert Message RNA Nitrogen Base (MRNA) to Protein (PM) and save Protein Key (PK)
6. Step 6: Create Playfair 5 X 5 matrix and use neural network generated key as key
7. Step 7: Use Playfair encryption process to get Protein Cypher (PC)
8. Step 8: Protein Ambiguity number as Protein Key (PK) and Protein Cypher (PC)

End

SIMULATION AND PERFORMANCE ANALYSIS

The proposed model is experimentally implemented and experimental result is given in this part. A comparison between the proposed model with bi – directional associative neural network key generation process and Genetic Algorithm with NW key generation process model is presented in this part since the plain format is almost the same. All of these models were implemented in a personal computer with following requirements Pentium core i7 processor, window 8 OS java was used to implement the modified model.

Encryption Time

The encryption time is the required time taken for the model to generate keys and encrypt a given plaintext to cipher text table given below compare the encryption time of the original systems with the modified system in (in milliseconds. the results show the two models takes similar time for the encryption because their main operation is both based on play fair cipher.

The Decryption Time is the required time taken for the model Decryption a given cipher text to plaintext. Table 2 below compares the Decryption Time of the original systems with the modified system in (in milliseconds. the results show the two models takes

similar time for the Decryption because their main operation is both based on play fair cipher.

Table 1. Comparison of encryption time with the characters from the modified model with the original scheme

Total number of Characters	Encryption Time	
	Modified Model	Original Scheme
500	0.0066003	0.0067002
1000	0.0100308	0.0100307
1500	0.0113393	0.0112294

Table 2. Comparison of encryption time with the characters from the modified model with the original scheme

Total number of Characters	Modified stem with BAMNN Key Generation original system with algo key gen	
	Modified Model	Original Scheme
500	0.0067	0.0057
1000	0.0202	0.0302
1500	0.0220	0.0230

Security Against Attacks

Brute force attack

A brute force attack uses trial-and-error to guess login information, encryption keys, or find a hidden web page. Hackers work through all possible combinations hoping to guess correctly. Since the space occupied by the keys is of multiples of 8-bits block, this form a space of n *2 ^{8} bi where n is the number of blocks. it's difficult to computationally calculate the key.

Known-plaintext attack

The **known-plaintext attack** (**KPA**) is an attack model for cryptanalysis where the attacker has access to both the plaintext (called a **crib**) and its encrypted version (ciphertext). These can be used to reveal further secret information such as secret keys and code books. In this context, even if the attacker recovers the key from the sets a different set of keys is generated forever execution freshly. Hence the proposed crypto system can withstand the known plaintext attack.

Differential cryptanalysis Attack

Differential cryptanalysis attack is a chosen plaintext attack where the attacker derives cipher text from a set of chosen plaintexts. This attack also fails because of fresh generation of keys which result in different cipher text each time (Table 3).

Table 3. Implementation of the system proposed in relation to the multiple attacks with modified systems

Attack	Encryption Time	
	Modified Model	Original Scheme
Brute-force	Prevention of attack	Prevention of attack
Ciphertext-only	Failure	Prevention of attack
Known-plaintext	Prevention of attack	Prevention of attack
Differential	Prevention of attack	Prevention of attack
Cryptanalysis	Prevention of attack	Prevention of attack

Achievement of CIA

Confidentiality is keeping information away from unauthorized people. In the proposed system this is achieved as all transmitted entities and parameters are encrypted.

Integrity

Integrity is the ability to ensure that data is accurate and remains unchanged. In the proposed system this is achieved because if a change happens in the cipher text it will affect the protein value and the DNA value, and the plaintext won't be able to be extracted.

Availability

It is important to ensure that the information concerned is always readily accessible to the authorized viewer. In the proposed system, this is achieved because it works with different plaintext size and types.

CONCLUSION

A Crypto system for encryption and decryption based bi-directional associative memory mapped for key generation is proposed. The plaintext use for

encryption undergoes several conversions and then finally encrypted using traditional play fair cipher. The proposed model or modified model survives some attack such as brute force and known plaintext attack. The modified model was compared with the original model based on encryption and decryption time and the result obtained shows that each model has equal encryption and decryption time. Also, CIA is achieved by the modified model.

REFERENCES

Abbasi, A. A., Mazinani, M., & Hosseini, R. (2020). Chaotic evolutionary-based image encryption using RNA codons and amino acid truth. *Optik, 223*, 165643. https://doi.org/10.1016/j.ijleo.2020.165643.

Alla, K., Praneetha, & Ramachandran, V. (2020). A novel encryption using genetic algorithms and quantum computing with roulette wheel algorithm for secret key generation. In *ICT Analysis and Applications* (Vol. 93, pp. 263–271). Springer. https://doi.org/10.1007/978-981-15-1465-4_26

Broumandnia, A. (2020). Image encryption algorithm based on the finite fields in chaotic maps. *Journal of Information Security and Applications, 53*, 102539. https://doi.org/10.1016/j.jisa.2020.102539.

Bajaj, A., & Sangwan, O. P. (2019). A systematic literature review of test case prioritization using genetic algorithms. *IEEE Access, 7*, 126355–126375. https://doi.org/10.1109/ACCESS.2019.2938884.

Basu, S., Karuppiah, M., & Nasipuri, M. (2019). Bio-inspired cryptosystem with DNA cryptography and neural networks. *Journal of Systems Architecture, 97*, 1–11. https://doi.org/10.1016/j.sysarc.2019.02.005.

Delman, B. (2004). *Genetic algorithms in cryptography* (Master's thesis). Rochester Institute of Technology. https://repository.rit.edu/theses/5456/

Sauber, A. M., Nasef, M. M., Sakr, A. S., & Geba, K. (2020). An efficient model to encrypt text and gray image based on amino acid chains. *The Egyptian Journal of Language Engineering, 7*(2), 20–31. https://journals.ekb.eg/article_112831.html

Sakr, A. S., Shams, M. Y., Mahmoud, A., & Zidan, M. (2022). Amino acid encryption method using genetic algorithm for key generation. *Computers, Materials & Continua, 70*(1), 123–134. https://doi.org/10.32604/cmc.2022.019455

Forouzan, B. A. (2017). *Cryptography and network security*. McGraw-Hill. Lima, P. M., Alves, M. V., Carvalho, L. K., & Moreira, M. V. (2017). Security against network attacks in supervisory control systems. *IFAC-Papers OnLine, 50*(1), 12333–12338. https://doi.org/10.1016/j.ifacol.2017.08.2005.

Mirjalili, S., Dong, J. S., Sadiq, A. S., & Faris, H. (2019). Genetic algorithm: Theory, literature review, and application in image reconstruction. In *Nature-Inspired Optimizers* (Vol. 811, pp. 69–85). Springer. https://doi.org/10.1007/978-3-030-12127-3_4.

Rutkowski, E., & Sheridan, H. (2020). Cryptanalysis of RSA: Integer prime factorization using genetic algorithms. In *2020 IEEE Congress on Evolutionary Computation* (pp. 1–8). IEEE. https://doi.org/10.1109/CEC48606.2020.9185804.

Zhang, Y., Liu, X., & Sun, M. (2020). DNA-based random key generation and management for OTP encryption. *Optik, 223*, 165643. https://doi.org/10.1016/j.ijleo.2020.165643.