Egyptian Journal of Language Engineering, Vol. 7, No. 2, 2020

An Efficient Model to Encrypt Text and Gray Image Based on Amino Acid Chains

Amr Mausad Sauber*[1], Mohammed M. Nasef*[2], Ahmed Saber Sakr*[3], Khaled Mohammed Geba**[4]

* *Department of Mathematics and Computer Science, Faculty of Science, Menoufia University, Egypt*

[1]amrmausad@computalityit.com

[2] mnasef81@yahoo.com

[3] a.ssakr@yahoo.com

** *Genetic Engineering and Molecular Biology Division, Department of Zoology, Faculty of Science, Menoufia University, Egypt*

[4]khaled.mohammed@icman.csic.es

Abstract: ***The main purpose of the data encryption process is the difficulty of understanding the content of the message with the difficulty of detecting the encryption mechanism. Therefore, in this paper, we proposed a new model of encryption based on the idea of encrypting text messages and gray images using amino acid chains. Amino acids are distinguished by being a series of alphabets represented by 20 characters and do not have a specific length. The main idea of this paper is to get an amino acid chain that contained encrypted message. To develop this model, we construct an artificial lookup table to encrypt any character of message to the amino acid chain, after that applying encryption process. The proposed model was applied on different kinds and sizes of messages, which proved the success of the main idea of the research, which is obtained amino acid chains with encrypted messages. The proposed model appears efficient in real time of encryption and extraction process compared with known methods. In the end, we compared the amino acids that we extract on the process of encrypting with internationally known amino acids and we found a similar ratio, which proves that the proposed model is effective in terms of increasing ambiguity of the encrypted message.***

Keywords: ***Amino Acid, Encryption, Decryption.***

1 INTRODUCTION

Digital media is transferred through the network. There are a lot of ways that can be used to transfer the digital media such as E-mail, Facebook, and Twitter …etc. When the data is transferred between two parties that are in the same and secure network, this does not cause a problem because it is a manageable network. But when the communication occurs through an open network, there are some problems that occur. The main problems are the opportunity for violation of the data ownership and jugglery data has increased the ease of copying digital data, it could lead to unauthorized copying extensively from it. The security of secret message must not only rely on the network security. Therefore, the data security must be taken into consideration which is one of the most important factors that used during the process of transferring data through the network, [1, 2]. Data security is used to protect the data from stealing or hacking it by unauthorized users.

2 BACKGROUND

A. Biological Background

Proteins are organic compounds formed of differential arrays of basic structural subunits named amino acids. Proteins vary in the number of amino acids they contain, being the maximum record until now is the 27,000 amino acid residues contained in the muscle sarcomeric proteins termed *titins*, [3]. The amino acids are basically formed of Carbon, Hydrogen, Oxygen and Nitrogen, with some of them having also other elements like Sulfur, Phosphorus, Iron, or Copper, [4]. All known proteins from the most ancient lines of bacteria up to the most complex organisms are formed from 20 amino acids, forming then the alphabet of cellular proteomes,[5]. Differentially joining these amino acids, different tissues within the same organism or different organisms can produce a vast variety of proteins (e.g. chlorophyll and Hemoglobin), including enzymes, hormones, oxygen-carrying molecules, antibodies, transporters, pigments, scales, hair, silk, milk, fish and snake poisons, antibiotic-degrading bacterial enzymes, etc. Some proteins, especially the ones involved in nutrition, are compressed macro-polymers of smaller peptides, i.e. collection of amino acids that perform differential functions, [6].

The basic structure of any amino acid is as shown in Figure 1, all centered around an α Carbon atom. The balance between the negativity of a carboxyl group (COO^-) and an amino group (NH_3) provides a neutral polarity for the amino acid in its simplest form. Two successive amino acids join each other by an amide bridge formed through dehydration reaction between the α amino group of one of them and the α carboxyl group from the other, yielding the peptide bond. Yet, amino acids differ in their sizes, polarities, structures and electric charges as a direct function of their side chains (the R groups). In this sense, for instance, alanine, valine, leucine, and isoleucine are all non-polar (hydrophobic) amino acids due to the presence of nonpolar, aliphatic R Groups in them. Methionine has a nonpolar thioether group in its side chain. Proline has an aliphatic, cyclic side chain with a secondary amino group that hinders the polypeptide chain formation. Phenylalanine, tyrosine, and tryptophan- all exhibit aromatic side chains making them relatively nonpolar (hydrophobic). On the other hand, the presence

of side chains that can for Hydrogen bonds with water make some amino acids water-soluble, i.e. polar (hydrophilic); such as serine and threonine (hydroxyl groups on their side chains), asparagine and glutamine (amide groups), and cysteine (sulfhydryl group), [5].

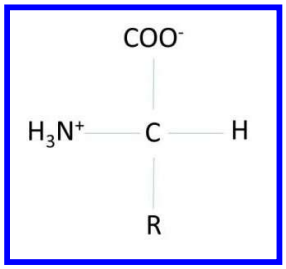


Figure 1: The Basic Structure of Amino Acids.

B. Cryptography

Cryptography is the study of encrypting or protecting the secret message from unauthorized persons. It is derived from the Greek words: kryptós, "hidden", and gráphe in, "to write" - or "hidden writing". The first evidence for the use of *cryptography* is found from 1900 B.C. in an inscription craved that has been done by an ancient Egyptian. The ancient Egyptian scribe used non-standard hieroglyphic symbols. This method is not believed to be a serious attempt in covert communication, but rather was an attempt to ambiguity, conspiracy and deceive onlooker who know how to read and write. From 500 to 600 B.C. Hebrew used a simple Substitution cipher (such as the at bash cipher). From 50 - 60 B.C. Julius Caesar used a form of encryption to secure the communications with the leaders of his armies in the war. Julius Caesar substituted the characters of the plain text with another character to create a cipher text. This substitution known as Caesar cipher. This is called a classical cryptography and it continued through history with many variations such as quantum cryptography, [7].

In cryptography, the secret message was scrambled and became gibberish to everyone. So, everyone knows that there is a secret message but cannot read it because it is not understandable, unreadable and opaque to anyone unless the decryption key is available. So, the decryption key must be very difficult to be known or used so that only the intended recipients who can remove the ambiguity and read the secret message, [7-9]. The cryptography technique processes are clarified in Fig 2.

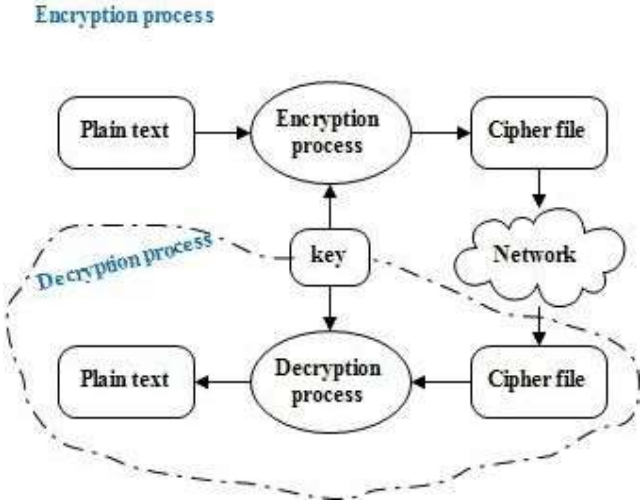


Figure 2: The General Diagram of Cryptography Technique

C. Related Work

Shiu et.al. [10] proposed three data hiding methods based on deoxyribonucleic acid sequence properties. Their work showed that deoxyribonucleic acid sequences have some features which can be used to hide data in it. In each method a reference deoxyribonucleic acid sequence C is selected as a container and the message M is inserted into it so that stego container is obtained. Stego container is then transferred to the destination that is able to identify and extract the message hidden in the stego container. Also, they proposed the hardiness and the insertion capacity analysis of the three proposed methods. Finally, their results showed a better performance of these methods compared to the performance of other methods with respect to different parameters such as capacity, payload and the number of bits per nucleotide (bpn).

Marwan et.al.,[11] presented a comprehensive analysis between the DNA-based playfair cipher, vigenere cipher, RSA and the AES ciphers, each combined with a DNA hiding technique. They conducted analysis reports for performance, diversity of each combined technique in terms of security, speed, hiding capacity in addition to both key size and data size. Moreover, they proposed a modification of the current combined DNA-based playfair cipher technique, which makes it not only simple

and fast but also provides a significantly higher hiding capacity and security. The conducted extensive experimental studies confirm such outstanding performance in comparison with all the discussed combined techniques. Atito et.al. [12], proposed a novel algorithm to communicate data securely. The proposed technique is a composition of both encryption and data hiding using some properties of Deoxyribonucleic Acid (DNA) sequences. Their proposed scheme consists mainly of two phases. In the first phase, the secret data is encrypted using a DNA and Amino Acids- Based Playfair cipher. While in the second phase the encrypted data is steganographically hidden into some reference DNA sequence using an insertion technique. The proposed algorithm can successfully work with any binary data since it is actually transformed into a sequence of DNA nucleotides using some binary conversion rule. Subsequently, these nucleotides are represented as an amino acid structure in order to pass through the specially designed Playfair Cipher and encrypt it into another DNA sequence. Then, this encrypted DNA data is randomly inserted into some reference DNA sequence to produce a faked DNA sequence with the encrypted data hidden. In order to recover the embedded secret data, the receiver can carry out the inverse process with the help of the both the secret key and the reference DNA sequence.

Jin-Shiuh Taur et.al. [13] proposed an improved algorithm named the Table Lookup Substitution Method (TLSM) to enhance the performance of an existing data hiding method called the substitution method. Moreover, a general form of the TLSM is discussed, which includes the original method as a special case.

Cheng Guo, et. al., [14] proposed a new DNA sequence-based data-hiding scheme. The proposed scheme can effectively hide two secret bits in a message by replacing one character. That approach can greatly improve the embedding capacity in data hiding.

Sushma R.B., et. al., [15] proposed, a technique to data steganography using DNA and Amino acid. Firstly, they converted the data to binary and then to DNA nitrogen bases. Secondly, then this DNA sequence is converted to amino acids. These amino acids are further converted to binary and embedded within cover image using 2-3-3 embedding technique and transmitted through the communication channel to the receiver.

Ghada Hamed et al., [16] proposed, an algorithm integrating between cryptography and steganography to achieve well secured and high capacity, that algorithm depends on molecular biology concepts. That algorithm is achieved by two phases. The first phase, the encryption process uses the DNA Playfair cipher. And the second phase, achieves a steganography process by exploiting the DNA mutations.

Md. Rafiul Biswas et. al., [17] proposed a technique for DNA cryptography based on dynamic mechanisms like “Dynamic DNA encoding” and “dynamic sequence table”. Firstly, to convert DNA sequences to 256 ASCII characters randomly. To obtain dynamism, positions of DNA base sequences are rearranged using a mathematical series. The process of encryption is carried out by transforming the plaintext into DNA using dynamic sequence table to assign them with ASCII characters. After that, encrypt data using an asymmetric cryptosystem after dividing to a finite number of chunks.

Xingyuan Wang et. al., [18] proposed a new technique to encrypt an image using chaotic, based on the coupled map lattices and DNA sequences. The initial values and control parameters of the coupled map lattice system and logistics map are served as keys and calculated using the SHA- 256 hash algorithm and the plaintext.

Kang Xuejing et. al., [19] proposed a new scheme to encrypt a color image based on DNA operations and spatiotemporal chaotic system is presented. Firstly, to hide the distribution information of the plain image, we convert the image into three DNA matrices. Then, construct a new matrix using a combination between DNA matrices and is permutated by a scramble matrix generated using mixed linear and nonlinear coupled map lattices (MLNCML) system.

3 PROPOSED MODEL

We have designed the proposed model in three phases. The first phase describes the idea of how to create an amino acid chain. The second phase describes the encryption process in detail. Finally, the third phase describes the extraction process of the message.

A. First Phase

In this phase, we describe the idea of Lookup table. From a study of amino acids we found that any amino acid can be represented by 20 alphabets. They are all alphabets except, J, U, O, X, B, and Z. Any message may contain any alphabet, special character and number. So, we have created a lookup table that we used to convert any character outside amino acid characters into amino acid domain, special characters and numbers are converted to the artificial amino acid chain.

For example

Table 1 shows how to replace special characters and letters that are not represented in amino acids with a series of artificial chains that were processed from letters found in amino acids. Table 2 shows how to replace the numbers from 0 to 9 with a series of artificial chains that were processed from letters found in amino acids

B. Second Phase "Encryption Process"

This process is done through the following steps.

1. As the proposed technique works on both text and images, it detects the message first to run the appropriate steps.
2. Determine the number of characters to be added before each letter of the message and this is the key to the process of adding “key1”.

TABLE I
LOOKUP TABLE FOR SPECIAL CHARACTERS

Character	Amino Acid Chain
J	ADEAD
O	ACEAC
U	ALEAL
X	WAEWA
B	YAEYA
Z	NAENA
:	CLLLN
.	FULSTPP
-	DAASH
,	CWMMMA
Space	MAEMA

TABLE II
LOOKUP TABLE FOR NUMBERS

Number	Amino Acid Chain
0	CERE
1	ENE
2	TWE
3	THREE
4	FEUR
5	FIVE
6	SICS
7	SEVEN
8	EIGHT
9	NINE

A - If the message is a text we do the following:

1. Each letter is studied separately if one of the twenty letters on which the amino acid depends on its composition is placed the letter as it is.
2. Otherwise, this character, number, or special character using the lookup table to replace by suitable artificial chain.
3. Step 1 is to be repeated for all letters until the message is finished.

B- If the message is an image we do the following:

1. Determine the size of the image.
2. Size of the image and each pixel's value can be represented by this code XXX to express the value of each pixel If the pixel's value = 5 is represented by 005, If the pixel's value = 12 is represented by 012, and If the pixel's value is 125 is represented as it is.
3. Each digit is replaced by a series of letters corresponding to it from the lookup table to turn the whole image into a series of letters composed of amino acid.
4. The image size is stored at the beginning of the message.
5. Step 4 is repeated until all pixels are finished.

C. Final phase "Extraction Process"

1. Search about artificial chains that are known to lookup table.
2. Replace these chains by corresponding letters, numbers or special characters from lookup table.
3. We must know the number of characters that were added before each letter in order to be able to extract "key1"
4. Extract characters are deleted by step 3
5. If after applying step 4, found other letters, this means that the message is a text and therefore the rest of the letters are placed in order with the results of step 2. Go to step 7
6. If after applying step 4, no found other letters, this means that the message is image because all values are numbers and here we apply the following:
   i. Divide these numbers into groups of 3 numbers
   ii. The first two sets of numbers are the width and height of the image
   iii. We extract the values of pixels from the groups by reversing the encryption process
7. Show the message

Figure3, figure4, and figure5 describe encrypted text message, encrypted image message, and extraction process respectively

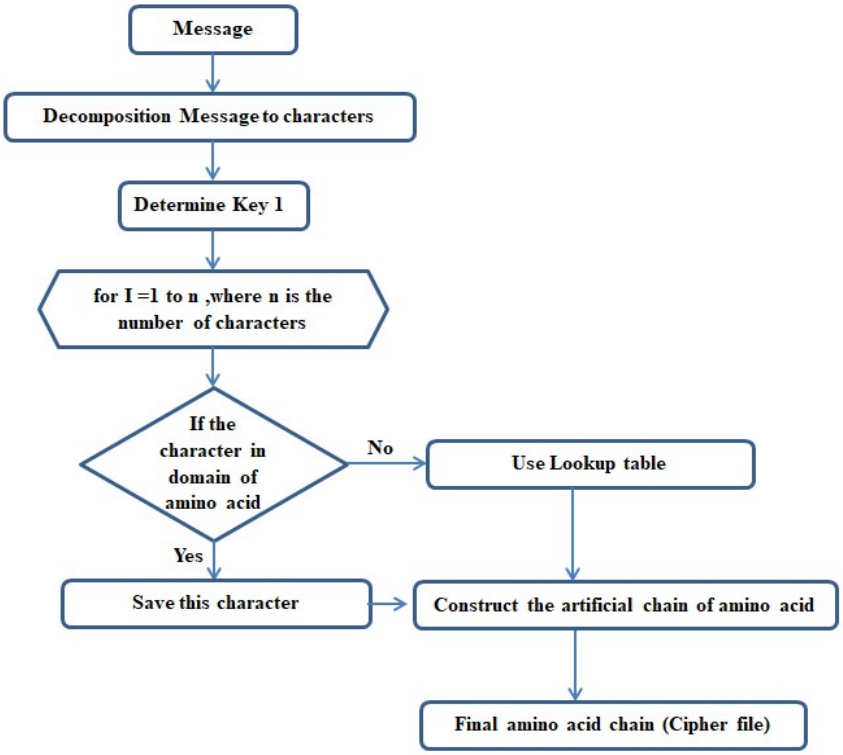


Figure 3: Model of Encrypted Text Message

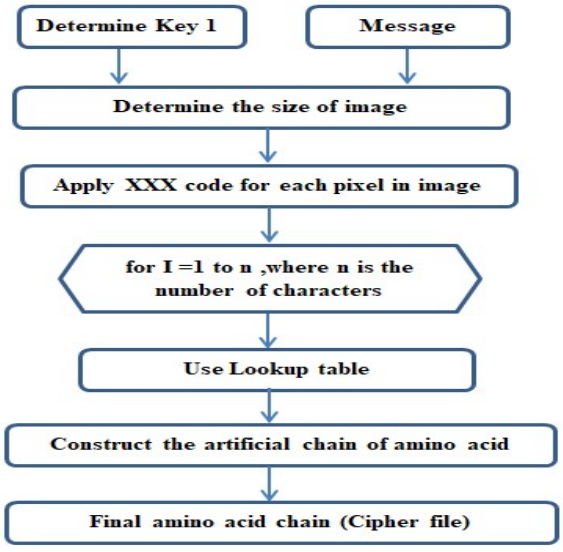


Figure 4: Model of Encrypted Image Message

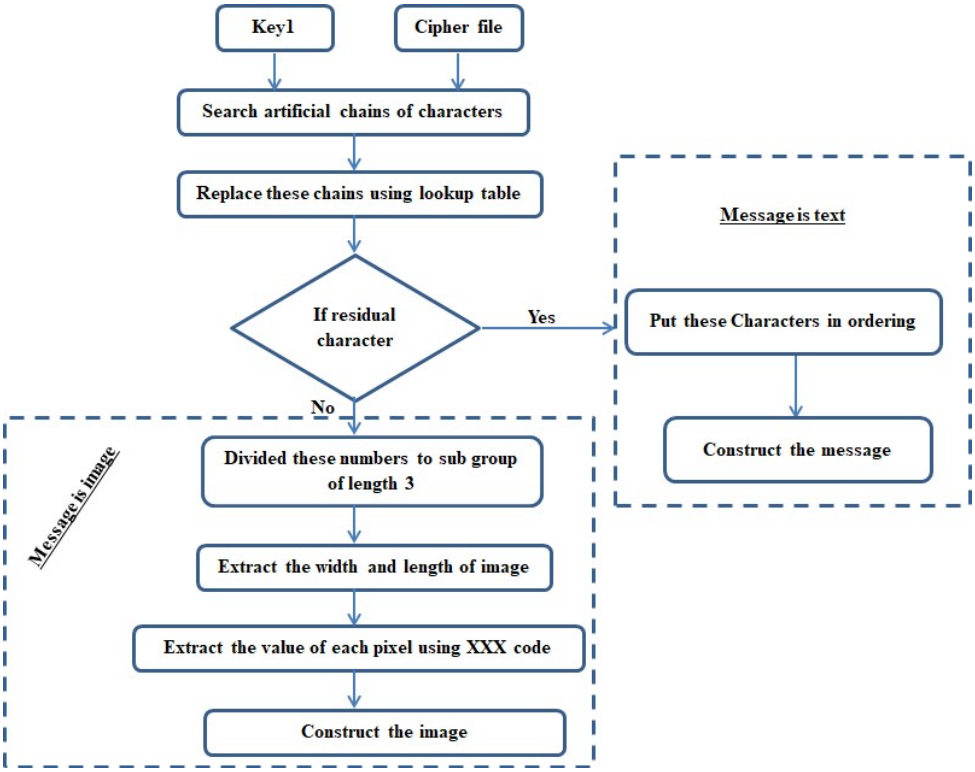


Figure 5: Model of Extraction Process

4 RESULTS

In this section we will present some of the results obtained from applying proposed model. Table 3 shows some text messages and images before and after encrypting them in the form of amino acid. Table 4, and table 5 shows size of the message, size amino acids and calculate the value of bpn. Table 6 presents comparing the similarity between the amino acids that were used in the process of encryption and amino acids known scientifically.

TABLE III: SOME EXAMPLES OF DIFFERENT MESSAGE AND RESULT AFTER APPLYING PROPOSED MODEL

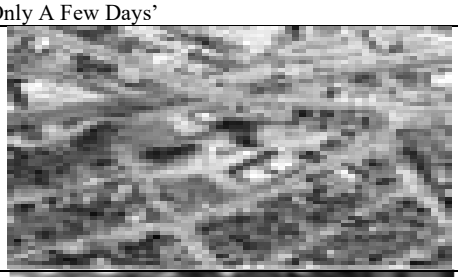
Part of message	Part of cipher file "Amino acid"
It Worked Perfectly Jbxzouj102165465 4646546546546546546546451 J	YPIMHTLAMAEMAISWERACEACQWRRWKS LEYCDVYMAEMAKDPMFEIGRSSFRKEGHCS RTTTLVCY
He Trafficker Identified Himself Only As Tom And Said He Was Based In Southeast Asia. Mr. Stiles Knew What Tom Was Hoping	YPTMHHLAEISMAEMAERTQWRRWASLFYCF VYIKDCMFKIGESSRRKMAEMAGHISRDTTEV CNNQT
Mr. Stiles Admitted Later. But He Was Eager To Bring Down Tom, Who Indicated That He Could Find Orangutans And Chimps With Only A Few Days'	YPMMHRLAFULSTPPISMAEMAERSQWTRWI SLLYCEVYSKDMAEMAMFAIGDSSMRKIGHT SRTTTEVC
	LWPQTKCWFKVDKGPIFPYGKKHFEYDQCPN HKFDHEVEVRKARFEDHNEKYPHQPEKDKYE HYIEGYAAYKGTVPAAEFKFEVQNAQF
	NSPIPKCWFTRDTVPIGPEMKDKFFPDPFPVFAI DCGHFYRACECIYFTDADHGESKHVVAPCKH HNFVEHEQSENSVDRKEIDKGAHRAWCIPPA MKKLCVKTAGKAGSIEFATAANCIE
	SWPYAKELFVRDNKPFEPICKAWFCSDQFPHC ANVCIHFHSADIAYFIGNATECEFFFMAADAH WIESAEYCQCFCPAYFCPQ
	ISPVEKSDFMFDENPGGPTAKFSFLGDQVPPQV NGKKRDTEAVRHGEGGAAEAHIWGVNAGIH QKGFLAWNGNEKLAACMHWQGEPASCHHHG HKAGCHYTGVFAINGIDK
	STPTTKKDFHQDIHPLAPIKKFFFSVDSPPKYK DVHFYETDKSTFPTHHWKWDEGWAHFKASH HHEEGKWEHRNENIKLDHRSERWANKAHEIV AQLILDAWTAMNI

TABLE IV: RESULT OF ENCRYPTION PROCESS "TEXT MESSAGE"

Example	Size of message	Size of Amino acid	bpn =(Size of message)/(Size of Amino acid)
Text1	504	4408	0.114338
Text 2	2888	12288	0.235026
Text 3	1400	5976	0.23427
Text 4	2016	8120	0.248276
Text 5	3728	15872	0.234879
Text 6	1464	6000	0.244
Text 7	2672	10960	0.243796
Text 8	2808	11736	0.239264
Text 9	3792	15328	0.24739
Text 10	3296	13696	0.240654

Table 4 shows the results of applying the proposed model to some text messages of different size. The table shows the size of each message and the size of the file after the encryption process 'amino acid' and the ratio of the message size to the amino acid size. Hence, the bpn ratio appears to vary by the alphabetical letters in the original message as the letters are encrypted according to the proposed model.

TABLE V: RESULTS OF ENCRYPTION PROCESS "IMAGE MESSAGE"

Image	Size of message	Size of Amino acid	bpn = (Size of message)/ (Size of Amino acid)
Satellite	6224	18688	0.333048
Baby	24656	73984	0.333261
Lena	98384	295168	0.333315
Cameraman	1179904	393296	0.333329
Baboon	1572944	4718848	0.333332

Table 5 shows the results of applying the proposed model to some gray images of different sizes. The table shows the size of each message and the size of the file after the encryption process 'amino acid' and the ratio of the message size of the amino acid. Hence it appears that the bpn ratio is almost constant, which is 0.333, due to the fact that the proposed model is based on the value of a pixel, which is numbered, and these numbers are encrypted in accordance with the proposed model.

TABLE VI: COMPARISON OF RESULTS OF PROPOSED MODEL WITH THE KNOWN AMINO ACIDS ON THE DATABASE (BLAST)

Cipher file contain	Highest identity with	Accession Number	Identity
Text1	leucine-rich repeats and immunoglobulin-like domains protein 1 isoform X1 [Homo sapiens]	XP_016861623.1	22%
Text2	four-helix bundle copper-binding protein [Solibacillus isronensis]	WP_079523817.1	33%
Text3	SCO family protein [Vibrio genomosp. F10]	WP_017036204.1	29%
Satellite image	ribonuclease E, partial [Halomonas salina]	WP_035599090.1	33%
Baby image	hypothetical protein EOQ54_01005 [Mesorhizobium sp.]	RWG08289.1	48%
Lena image	PREDICTED: fibulin-2-like [Sinocyclocheilus grahami]	XP_016088093.1	42%
Cameraman image	hypothetical protein Csa_6G197210 [Cucumis sativus]	KGN47190.1	27%
Baboon image	hypothetical protein [Actinomadura oligospora]	WP_026415800.1	38%

Table 6 presents the results of comparing some of the amino acids extracted from the encryption process with a global database containing real amino acids (Blast) to determine the extent to which these acids match. The table shows the name of the amino acid similar to the output of the encryption and the identical ratio.

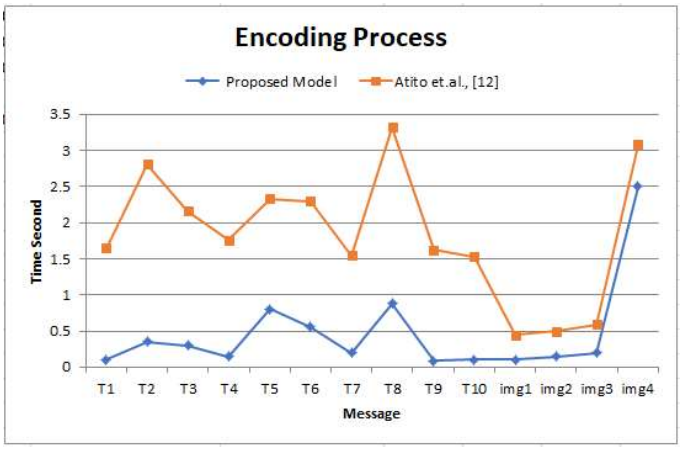


Figure 6: Comparison Time of Encoding Process between Proposed Model and Atito et. al., [12]

Figure 6 shows the real-time comparison of the process of encryption on a set of text messages and gray images. The figure shows that the time taken for the encryption process of the proposed model is less than that used in Atito et. al., [12].

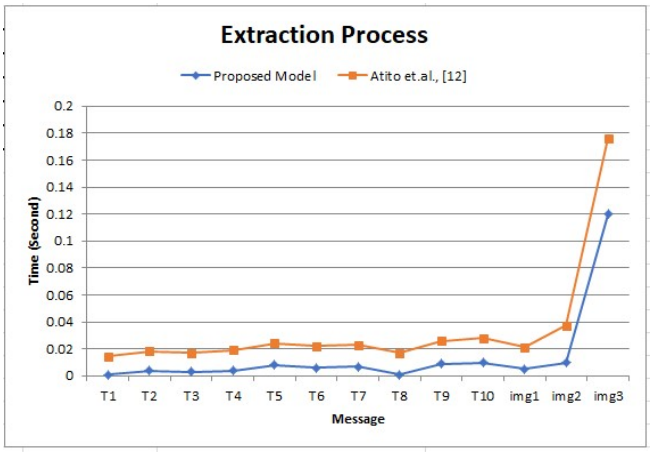


Figure 7: Comparison Time of Extraction Process between Proposed Model and Atito et. al., [12]

Figure 7 shows the real-time comparison of the process of extracting text messages and gray images that have already been encrypted from the encrypted file. The figure shows that the time taken for the extraction of the proposed model is less than that used in Atito et. al., [12].

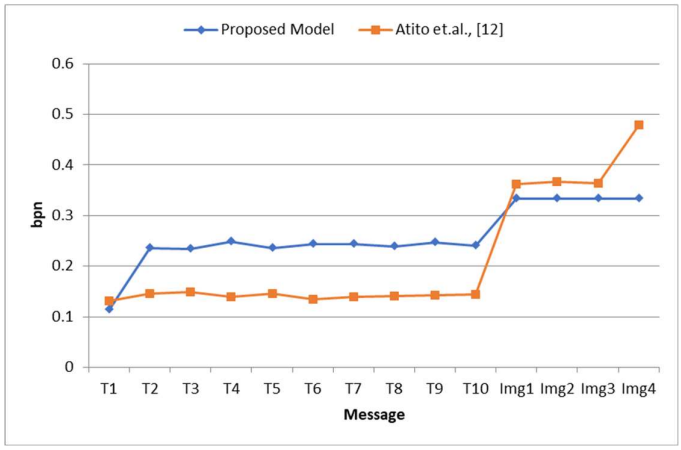


Figure 8: Comparison bpn of Extraction Process between Proposed Model and Atito et. al., [12]

Figure 8 demonstrated that bpn of the proposed model has better values than atito et al., [12] in text messages, but in gray images the other method is better than proposed model, because the proposed model deal with the pixel value as three different numbers so it take much bpn but atito et al., [12] deal with the pixel value as one number.

5 CONCLUSION

In this paper, we proposed a model to encrypt both text and gray images. It depends on the idea of forming chains of amino acids as these chains depend on their composition on a set of alphabets and they are 20 characters. A complementary group of characters is added to perform a lookup table to all possible characters. Since there is no specific restriction for the length of the amino acid chain, this is to be utilized to encrypt any message into a chain of amino acids. The results of the proposed model were satisfying in terms of both time and bpn, as the results shows the proposed model outperforms other models in times as well as the bpn in text messages and some gray images. Also to measure the efficiency of the proposed model in terms of the ambiguity surrounding the encrypted message, the encrypted messages had been compared with original ones and the similarity ratio has been displayed, showing that the percentage of ambiguity on encrypted messages is increased.

REFERENCES

[1] Djebbar, B. Ayad, K. Meraim and H. Hamam, "Comparative study of digital audio steganography techniques", *EURASIP Journal on Audio, Speech, and Music Processing,* vol. 2012, no. 1, p. 25, 2012.

[2] W. Bender, D. Gruhl, N. Morimoto and A. Lu, *"Techniques for data hiding", IBM Syst. J.,* vol. 35, no. 34, pp. 313- 336, 1996.

[3] Fulton, A. B., and Isaacs, W. B.," Titin, a huge, elastic sarcomeric protein with a probable role in morphogenesis". *Bioessays*, 13(4), 157-161., 1991

[4] Bukya A. and Poongodi Vijayakumar T., "Food Proteomics. In: Advances in Food Science and Nutrition". *Ed. Yashi Srivastava. Science and Education Development Institute, Nigeria.* P. 77, 2013

[5] Boyle J," Amino Acids, Peptides, and Proteins. In: Lehninger Principles of Biochemistry", *Fourth Edition - David L. Nelson, Michael M. Cox; W.H. Freeman and Company, New York, USA PP.* 76-85, 2015.

[6] K. Mohammed-Geba, F. Arrutia, H. Do-Huu, Y. J. Borrell, A. Galal-Khallaf, A. Ardura, Francisco A. Rierac and Eva Garcia-Vazquez*," VY6, a β-lactoglobulin-derived peptide, altered metabolic lipid pathways in the zebra fish liver", Food Funct.*_2016 Apr; 7(4):1968-74. doi: 10.1039/c6fo00003g.

[7] A. Raphael and D. Sundaram, "Cryptography and Steganography – A Survey", *International Journal of Computer Technology and Applications,* vol. 2, no. 3, pp. 626-630, 2011.

[8] Z. V. Patel and S. A. Gadhiya, "A Survey Paper on Steganography and Cryptography", *International Multidisciplinary Research Journal (RHIMRJ),* vol. 2, no. 5, pp. 1-5, 2015.

[9] K. P. Adhiya and S. A. Patil, "Hiding Text in Audio Using LSB Based Steganography", *Information and Knowledge Management*, vol. 2, no. 3, pp. 8- 14, 2012.

[10] H.J. Shiu, K.L. Ng, J.F. Fang, R.C.T. Lee, and C.H. Huang, "Data hiding methods based upon DNA sequences", Information Sciences vol. 180, pp. 2196–2208, 2010.

[11] Samiha Marwan, Ahmed Shawish, and Khaled Nagaty, "DNA-based cryptographic methods for data hiding in DNA media", *Biosystems* vol. 150, pp 110-118, 2016.

[12] Ahmed Atito, Amal Khalifa, and SZ Rida, "DNA-based data encryption and hiding using playfair and insertion techniques", *Journal of Communications and Computer Engineering*, vol. 3, issue 2, pp 44-49, 2012.
[13] Jin-Shiuh Taur, Heng-Yi Lin, Hsin-Lun Lee and Chin-Wang Tao, "Data Hiding In DNA Sequences Based on Table Lookup Substitution", *International Journal of Innovative Computing, Information and Control, Volume 8, Number 10(A),* pp. 6585–6598, October 2012.
[14] Cheng Guo, Chin-Chen Chang and Zhi-Hui Wang, "A New Data Hiding Scheme Based on DNA Sequence", *International Journal of Innovative Computing, Information and Control Volume 8, Number 1(A),* pp. 139–149, January 2012.
[15] Sushma R.B. , Namitha M.V. , Manjula G.R. , Sayyed Johar ,and Hiriyanna G.S, "DNA Based Steganography using 2-3-3 Technique*", 2019 International Conference on Data Science and Communication (IconDSC), IEEE, DOI:* 10.1109/IconDSC.2019.8816945.
[16] Ghada Hamed, Mohammed Marey, Safaa Amin El-Sayed, Mohamed Fahmy Tolba, "Hybrid, Randomized and High Capacity Conservative Mutations DNA-Based Steganography for Large Sized Data", *BioSystems, doi:10.1016/j.biosystems.*2018.03.003.
[17] Md. Rafiul Biswas, Kazi Md. Rokibul Alam, Shinsuke Tamura, Yasuhiko Morimoto, "A technique for DNA cryptography based on dynamic mechanisms", *Journal of Information Security and Applications,* 48 (2019) 102363, /doi.org/10.1016/j.jisa.2019.102363.
[18] Xingyuan Wang, Yu Wang, Xiaoqiang Zhu, Chao Luo, "A novel chaotic algorithm for image encryption utilizing one-time pad based on pixel level and DNA level*", Optics and Lasers in Engineering 125 (2020) 105851, doi.org/10.1016/j.optlaseng*.2019.105851.
[19] Kang Xuejing, Guo Zihui, "A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system", *Signal Processing: Image Communication 80 (2020) 115670, doi.org/10.1016/j.image*.2019.115670

BIOGRAPHY

Amr Mausad Sauber is an Assistant Professor of Computer Science in the Faculty of Science, Menoufia University. He received his M.Sc. and Ph.D. Degree in Computer Science from Faculty of Science, Menoufia University. His research interests Database systems, and machine learning. He is a member of the Egyptian Society of Language Engineering. He is the head of the IT unit in the Faculty of Science, Menoufia University. He is a Treasurer of the Society of Basic and Applied Science at Menoufia University.

Mohammed M. Nasef is an Assistant Professor of Computer Science in the Faculty of Science, Menoufia University. He received his M.Sc and Ph.D. Degree in Computer Science from Faculty of Science, Menoufia University, Egypt in 2007, and 2011, respectively. His research interests include artificial intelligence, audio steganography, audio classification, and machine learning. He is a member of the Egyptian Society of Language Engineering. He is a secretary of the Society of Basic and Applied Science at Menoufia University. He is a member of the editor board of the international journal of computer network and information security from 2015 until now.

Ahmed Saber Sakr received his Ph.D. in computer science in the faculty of science, Menoufia University. He is now a lecturer of computer science. His main interest is in cloud computing, data security and big data .He is Certified Trainer from IBCT. He is a chairman of the society of basic and applied Science at Menoufia University.

Khaled Mohammed Geba received his Ph.D. and MS.c. Molecular Biology, University of Cádiz in Spain; He is a Molecular Biologist with a wide experience in teaching and research in molecular biology, biotechnology, population genetics, genetic diversity and molecular mechanisms of bio-production and adaptation in different environments. He is a Membership of the Marine Biological Association of the UK (Professional Member), World Aquaculture Society, USA, Aquatic Ecosystem Health and Management, Canada, Egyptian Society of Natural Toxins, Suez Canal University, and The Egyptian Journal of Experimental Biology, Tanta University

نموذج فعال لتشفير النص والصورة الرمادية مبني علي سلاسل الأحماض الأمينية

عمرو مسعد صابر* [1] ، محمد مصطفى ناصف * [2] ، أحمد صابر صقر * [3] ، خالد محمد جبه ** [4]
*قسم الرياضيات وعلوم الحاسب - كلية العلوم - جامعة المنوفية – مصر
[1]amrmausad@computalityit.com
[2]mnasef81@yahoo.com
[3]a.ssakr@yahoo.com
** شعبة الهندسة الوراثية والبيولوجيا الجزيئية - قسم علم الحيوان - كلية العلوم - جامعة المنوفية - مصر
[4]khaled.mohammed@icman.csic.es

الملخص:
إن الغرض الرئيسي من عملية تشفير البيانات هو صعوبة فهم محتوى الرسالة وصعوبة اكتشاف آلية التشفير. لذلك ، اقترحنا في هذه الورقة نموذجًا جديدًا للتشفير بناءً على فكرة تشفير الرسائل النصية والصور الرمادية باستخدام سلاسل الأحماض الأمينية. تتميز الأحماض الأمينية بكونها سلسلة من الحروف الأبجدية ممثلة بـ 20 حرفًا وليس لها طول محدد. الفكرة الرئيسية لهذه الورقة هي الحصول على سلسلة حمض أميني تحتوي على رسالة مشفرة.
في هذا النموذج ، نقوم ببناء جدول بحث اصطناعي لتشفير أي حرف من الرسالة إلى سلسلة الأحماض الأمينية ، بعد ذلك تطبيق عملية التشفير. تم تطبيق النموذج المقترح على أنواع وأحجام مختلفة من الرسائل ، والتي أثبتت نجاح الفكرة الرئيسية للبحث . أظهر النموذج المقترح فاعليه في الوقت الحقيقي لعملية التشفير والاستخراج مقارنة بالطرق المعروفة. في النهاية قمنا بمقارنة الأحماض الأمينية التي نستخرجها من عملية التشفير بالأحماض الأمينية المعروفة دوليًا ووجدنا نسبة تشابه ، مما يثبت أن النموذج المقترح فعال من حيث زيادة الغموض على الرسالة المشفرة.

الكلمات االمفتاحيه:
الأحماض الأمينية ، التشفير ، التشفير ، فك التشفير