Годишник Телекомуникации 2022, том 9, с. 35-44

Yearbook Telecommunications 2022, vol. 9, p. 35-44

eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii

DOI: https://doi.org/10.33919/YTelecomm.22.9.3

AN ALGORITHM FOR STEGANOGRAPHIC EMBEDDING OF ENCRYPTED FILES IN RASTER IMAGES

Yoana Ivanova

Abstract: The aim of this paper is proposing a method for the application of algorithms for hiding an encrypted file inside of a digital image for cybersecurity purposes. The originality of the method is expressed in the possibility of studying the mathematical algorithms for creating computer graphics. The development of a comprehensive algorithm should contribute to the practical realization of the method proposed. It emphasizes on built-in algorithms in software systems for creating computer graphics and the advantages of steganographic embedding by opensource products that hides any archive file in a digital image. Its application contribution is supported by practical examples of software hiding and archiving an encrypted file in a graphic image.

Keywords: Vigenere cipher, affine transformations, Bezier curves, vector and raster steganography.

1. INTRODUCTION

The main purpose of the author is to propose a reliable algorithm of steps including symmetric encryption of a message and embedding it inside of a digital image using a steganography software. Actually, the hybrid method of consequently application of encryption and steganography is used in practice, although the encryption is more popular than steganography. The encrypted files are embedded in raster or vector digital images which should Srtebe preliminary taken or created using a specialized software. Especially for steganographic applications it is not recommended the graphic image to be downloaded for free from the Internet due to the risk they already contain a watermark.

Conceptually the main difference between cryptography and steganography is expressed in their aims. While cryptography makes the information in a message unreadable, steganography hides the message itself. In this sense steganographic techniques ensure a higher level of security compared to encryption and compression while being compatible with them under certain technical requirements.

As it is known, the asymmetric cryptographic algorithms use different keys for encryption and decryption to establish a secure session between a client and a server while the symmetric cryptographic algorithms are responsible for the data transfer during the session established. Each of the two main types of algorithms has their advantages. Actually, the asymmetric cryptographic algorithms are much more resistant to cyber impacts compared to the symmetric ones due to their high level of complexity. But precisely because of their lower complexity the symmetric algorithms are performed in a shorter time for ciphering and deciphering than the asymmetric ones.

This selection of separately applicable algorithms and their collaborative application aims to show a possible optimization of the overall process related to ensuring security of information during its storage and transmission. As it is known the cryptographic and security protocol TLS (Transport Layer Security) or SSL (Secure Sockets Layer) uses asymmetric and symmetric encryption to provide two main criteria of methodology CIA (CIA triad - confidentiality, integrity and availability) – confidentiality and integrity of data-in-transit realizing a high level of protected communication between two parties.

For example, in security and defence are used the computer security standard Federal Information Processing Standard Publication (FIPS 140-2) and TCG-Opal self-encrypting drives (SEDs), which use AES (Advanced Encryption Standard) encryption algorithms [1] to strengthen security of classified information.

The content of the paper is structured in three sections. **Section 2** includes a comparative analysis of main cryptographic algorithms by specific criteria and emphasizes on the advantages of Vigenere cipher that is reasonable because of its applications. **Section 3** explains the specific characteristics of the raster/vector computer graphics (RCG/VCG) and the mathematical apparatus on which VCG is based, as well as affine transformations related to digital objects (translation, rotation and scaling). A practical example of embedding an encrypted file in a digital image using steganography software in described in **Section 4.**

2. A COMPARATIVE ANALYSIS OF CRYPTOGRAPHIC ALGORITHMS

The main steps in the algorithm proposed by the author are presented in the diagram shown in Figure 1. It is recommended the compression to be performed before the encryption. One of the most effective algorithms for a reversible lossless compression is the Huffman coding.

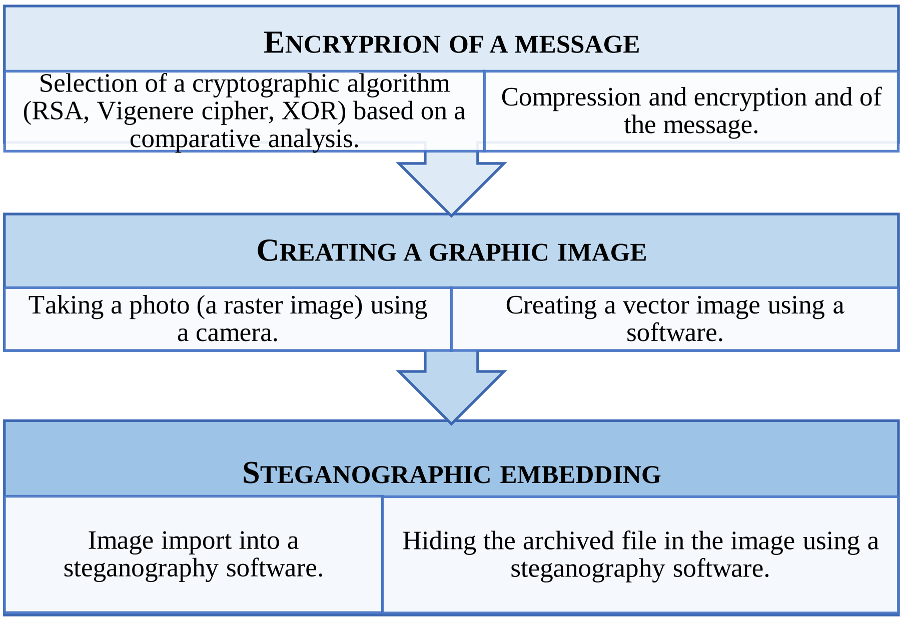

ENCRYPRION OF A MESSAGE
Selection of a cryptographic algorithm (RSA, Vigenere cipher, XOR) based on a comparative analysis.
Compression and encryption and of the message.
CREATING A GRAPHIC IMAGE
Taking a photo (a raster image) using a camera.
Creating a vector image using a software.
STEGANOGRAPHIC EMBEDDING
Image import into a steganography software.
Hiding the archived file in the image using a steganography software.

Fig. 1. An algorithm for steganographic embedding of encrypted files.

A combination of a public key encryption using the asymmetric algorithm RSA (Rivest–Shamir–Adleman) and the Vigenere cipher is characterized by reliability and efficiency in providing protection [2]. In terms of security the Vigenere cipher requires a no shorter key length than the plaintext length to reduce its vulnerability to cyberattacks. In that sense the RSA algorithm is more resilient except under the influence of extraordinary factors [3].

The Vigenere cipher is a classical method of encryption that is applicable for different purposes individually or in combination with other cryptographic algorithms. For encrypting a text is used a special table called the Vigenere cipher table or Vigenere square. In the Vigenere table (VCT) each letter in the plaintext (first column in VCT) is replaced by a letter corresponding to the key letter (first row in VCT). It is easily accessible in many sources because of the popularity of this algorithm.

This polyalphabetic algorithm is characterized by the following advantages:

- ***optimal level of complexity*** – as it was explained in the introduction to the article, if an algorithm is extremely complex, this could be taken as a disadvantage in terms of optimizing the duration of encryption and decryption. In this sense the Vigenere cipher is characterized by sufficient complexity being at the same time more complex compared to other substitution algorithms such as the Caesar cipher.

eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii

DOI: https://doi.org/10.33919/YTelecomm.22.9.3

- ***invulnerability to frequency analysis*** – the frequency of the most used letters in the encrypted text is different compared to that of the most commonly used letters in the plaintext due to this mechanism: *"the number of places a letter in the plaintext message is shifted in the alphabet changes for each letter in the plaintext message"* [4].
- ***compatibility with the other algorithms*** – for example a collaborative encryption with the RSA algorithm is feasible and reasonable in order to achieve a better level of security.
- ***advanced applications*** – it is very suitable especially for secure transmission over SMS technology, VPN (Virtual Private Network), microprocessor software security, image security, communications and etc. [5].

An example of encryption using the Vigenere cipher table (VCT) [6] and ASCII conversion chart [7] is demonstrated in Table 1. There are different variants of encryption using the ASCII table, but the most common is the binary code to be substituted with letters from the alphabet or symbols in the column ASCII of the conversion.

Another example of such a conversion is practiced in exclusive-OR (XOR) [8] encryption that is applicable in DES and Triple DES algorithms. Besides, in this kind of encryption the process of ciphering continues with five new steps as follows:

- ***converting the binary code obtained by compression in a new string of letters using the ASCII table.***
- ***selection of a cryptographic key with the same length as the string of letters;***
- ***converting the key in a binary code using the ASCII table;***
- ***performing the XOR operation on the two binary codes;***
- ***converting the binary code obtained after the XOR operation in a new string of letters using ASCII table.***

In fact, this algorithm is characterized by a high level of complexity due to the several encryptions despite the use of a single key for encryption and decryption. If the results of an empirical research prove that this method causes decryption difficulties and prolongs the decryption time it could be replaced with the Vigenere cipher in order to optimize the encryption process. In this case the five steps from the previous method are reduced to three as follows:

- ***converting the binary code obtained by compression in a new string of letters using the ASCII table.***
- ***selection of a cryptographic key with the same length as the string of letters;***
- ***substitution of the letters in the string obtained by compression with letters from the Vigenere cipher table.***

In the row "XOR" of Table 1 are calculated the binary codes using the table of the logical operation XOR.

Table 1. Encryption using the Vigenere cipher.

Plaintext	**C**	**I**	**P**	**H**	**E**	**R**
Key	C	R	Y	P	T	O
Encrypted text	**E**	**Z**	**N**	**W**	**X**	**F**
Plaintext in binary	01000011	01001001	01010000	01001000	01000101	01010010
Key in binary	01000011	01010010	01011001	01010000	01010100	01001111
XOR	00000000	00011011	00001001	00011000	00010001	00011101
DEC	0	27	9	24	17	29
ASCII	**NUL**	**ESC**	**HT**	**CAN**	**DC1**	**GS**

Actually, the advanced methods of information protection are related to the joint application of encryption and compression algorithms, as it is recommended the compression to precede the encryption, because of the higher resilience in this case [9].

An example of lossless compression using Huffman coding [10] is demonstrated for the string of letters **AVATAR**. The frequency table is shown in Table 2, the tree of Huffman and the resulting string encoded into binary are displayed respectively in Figure 2 and Table 2. It should be noted that after compression the size of the string decreases more than 4 times. Table 3 contains also the corresponding letters from the ASCII table for the binary code of the string.

Table 2. An example of text compression by Huffman coding

Letter		***Frequency***	
A		3	
V		1	
T		1	
R		1	
Total characters	***Before compression***	6 bytes	48 bites
	After compression	1,375 bytes	11 bites

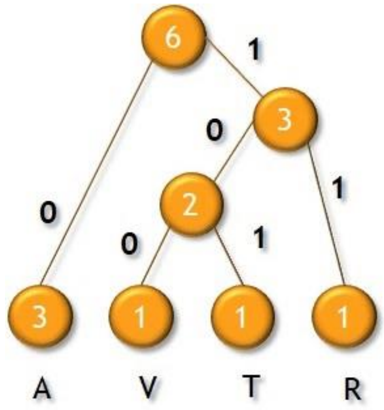


Fig. 2. The tree of Huffman built for the string “AVATAR”.

Table 3. The binary code of the string after the compression and a simple encryption.

String	***A***	***V***	***A***	***T***	***A***	***R***	
Binary codes	0	100	0	101	0	11	
Blocks of 8 bits			01000101			011	
Decimal			69			0	3
ASCII table			E			NUL	ETX

If this is the end step of the transformation the original string could be restored quickly under certain conditions such as small length of the string, correct information for the tree and the binary code. Actually, the reversibility of compression is an advantage if the integrity of the original information must be preserved. But if this information is confidential then there is a security risk because the mechanism of compression is not equivalent to encryption. Therefore, the binary code received should be converted in a different string of letters compared to the plaintext.

In conclusion of this section devoted to applicable in practice encryption and compression algorithms the author summarizes the results of a comparative analysis of cryptographic algorithms AES-256 and TripleDES (168 bits for keys K1, K2 and K3) presented in Table 4. This analysis is based on three important criteria: speed; complexity based on the key length; level of security; compatibility with encryption software; resilience to a differential linear interpolation (differential cryptanalysis). The rating scale established for each criterion is as follows: 1 – low; 2 – middle; 3 – high.

Table 4. Comparative analysis of AES and Triple DES.

Criteria	*AES-256*	*TripleDES*
Speed	3	1
Complexity	3	2
Security	3	2
Compatibility	3	3
Resilience	3	2
Average	**3**	**2**

The vulnerability of TripleDES to differential cryptanalysis is expressed in the risk of detecting the difference between related open texts that are encrypted. *“The plaintext can differ by a few bits.”* This kind of attack is classified as *“adaptive attack with selected open text”*. The key is unknown for the attacker, who has selected *“the plaintext to be encrypted and then encrypts related plaintexts.”* This statistical analysis aims to detect *“signs of non-randomness”* in the encrypted texts, seeking for areas in which they differ [11].

3. FUNDAMENTAL MATHEMATICAL ALGORITHMS AND AFFINE TRANSFORMATIONS IN COMPUTER GRAPHICS

Creating proprietary digital images for steganographic embedding is important to reduce potential risks of using copyrighted images that have already imported an invisible watermark.

The main difference between raster and vector computer graphics (CG) is expressed in the way of building. As it is known the raster images are based on a 2D matrix of pixels containing information for the color. Vector CG is based on Bezier curves defined by n+1 control points and surfaces. A digital object with a certain shape is drawn by changing the position of the control points of the curve which is mathematically described especially by polynomial functions named after Prof. Sergei Bernstein that can be represented as follows:

$$P\ (u) = \sum_{i=0}^{n} P_i \cdot B_{n,i}(u) \qquad (1)$$

The coordinate functions of the radius vector of a point of the curve are polynomials of a real argument. $B_{n,i}(u)$ are $n+1$ basic polynomial functions of a real variable $u \in [0,\ 1]$. According to the degree of the curve n the one-dimensional basis function is expressed by the following equation [12]:

$$B_{n,i}(u) = \frac{n!}{i!(n-i)!} u^i (1-u)^{n-i}, \qquad (2)$$

where i are $n+1$ coefficients of the polynomial which are real numbers (0, 1, …n) [13].

During the creation of vector CG in a software environment it is possible to add new points on the Bezier curve. The coordinates of these points can be calculated using the algorithm of Paul De Casteljau's (De Casteljau's Algorithm) by multiple linear interpolation.

If a point C divides the segment AB, as the ratio AC/AB = u, then the position of point C is determined by the equation:

$$C = A + u.(B - A) = A + u.B - u.A = A\,(1 - u) + u.B \qquad (3)$$

For example, if the coordinates of the control points P_0, P_1, P_2 and P_3 and the value of u are known, the coordinates of the point $P_{3,0}$ can be calculated using the scheme shown in Figure 3 by performing the following steps:

- the coordinates x and y of each two adjacent control points are multiplied by (1 - u), where there is a black arrow (down) and respectively by u, where there is a blue arrow (up).
- the values obtained are summed.

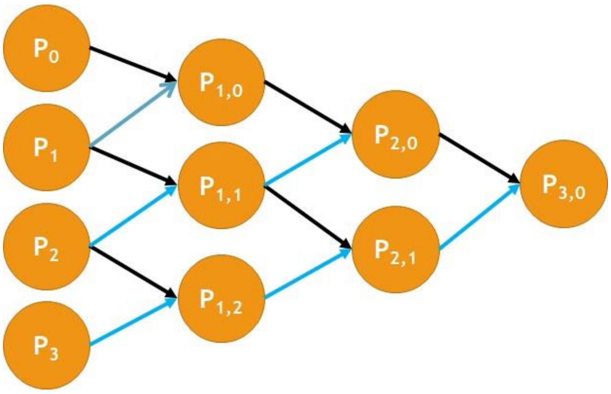


Fig. 3. Application of De Castello's algorithm for four control points.

The affine transformations allow the completed digital objects to be moved by a translation, rotated by a rotation or resized by scaling, preserving lines, parallelism and proportions. Each geometric transformation can be represented in matrix form as follows:

- ***translation*** - the displacements dx and dy are added to the original coordinates of each point. The new coordinates (x', y') of the point after the translation are:

$$x' = x + dx;\; y' = y + dy \qquad (4)$$

$$\begin{bmatrix} x + dx \\ y + dy \end{bmatrix} = \begin{bmatrix} dx \\ dy \end{bmatrix} + \begin{bmatrix} x \\ y \end{bmatrix} \qquad (5)$$

In order to multiply the matrices, they need to be transformed in homogeneous coordinates by adding a homogeneous point laying on a plane (w = 1) to each vector or point [14]. The homogeneous point of translation is:

$$P' = \mathrm{T}\,(dx, dy).\,P = \begin{bmatrix} 1 & 0 & dx \\ 0 & 1 & dy \\ 0 & 0 & 1 \end{bmatrix} . \begin{bmatrix} x \\ y \\ 1 \end{bmatrix} \qquad (6)$$

- ***rotation*** - all points that describe the object are placed in a new position by rotating them to a predefined angle and axis of rotation. the object moves along an arc of a circle in the plane xy on which the axis of rotation is perpendicular. The point at which the axis of rotation intersects the plane is called reference point. If the reference point coincides with the origin of the coordinate system and the rotation R of the object is at an angle θ, then:

$$P' = P.R \qquad (7)$$

$$x' = x.cos(\theta) - y.sin(\theta) \qquad (8)$$

$$y' = x.sin(\theta) + y.cos(\theta) \qquad (9)$$

The rotation of a point lying on the abscissa and the ordinate is respectively:

$$R(1;0) = (cos(\theta), sin(\theta)) \qquad (10)$$

$$(0;1) = (cos(\theta+\pi/2), sin(\theta + \pi/2)) \qquad (11)$$

The rotation matrix has the following form:

$$R = \begin{bmatrix} cos(\theta) & cos(\theta + \pi/2) \\ sin(\theta) & sin(\theta + \pi/2) \end{bmatrix} = \begin{bmatrix} cos(\theta) & -sin(\theta) \\ sin(\theta) & cos(\theta) \end{bmatrix} \qquad (12)$$

- ***scaling*** – scaling to the origin of the coordinate system of a homogeneous point and the matrix multiplication are:

$$P' = S(Sx, Sy).P = \begin{bmatrix} Sx & 0 & 0 \\ 0 & Sy & 0 \\ 0 & 0 & 1 \end{bmatrix} . \begin{bmatrix} x \\ y \\ 1 \end{bmatrix} \qquad (13)$$

4. A PRACTICAL REALIZATION OF THE ALGORITHM FOR IMAGE STEGANOGRAPHIC EMBEDDING OF ENCRYPTED FILES

(LSB) Least Significant Bits and MSB (Most Significant Bits) are classical steganographic techniques for substitution respectively of the lowest and the highest bits of the image with bits of the encrypted message. Therefore, the two techniques can be combined into algorithms embedded in software products.

The empirical part of this research is divided into several stages according to the scheme presented in Section 2 (Figure 1).

4.1.Encryption of a message using a software product

For example, Disk Encryptor and Vera Crypt are suitable variants to encrypt and decrypt a disk or partitions of the disk not only because the open source, but also due to the possibility to select an encryption algorithm which is important for a subsequent assessment and analysis of the experimental results.

In this case the author has selected two encryption products which are suitable for a comparative analysis of the results because they both use highly secured encryption by AES (Advanced Encryption Standard) symmetric algorithm:

- ***7-zip*** – uses 256-bit key AES. It is chosen not because of its popularity but because the aim is to encrypt and compress a file. In fact, this software is widely used for compression, but has its own Encryption Section.
- ***CryptoForge*** – also uses AES-256, but it is possible to encrypt with TripleDES, Blowfish and Gost.

The encryption processes for the file **AVATAR_plaintext.txt** using 7-zip and CryptoForge are presented in Figures 4. In 7-zip there is an option to encrypt the file name. It is interesting to note that CryptoForge supports various types of compression including 7-zip, but it is not acceptable to compress already compressed files. The options to compress before encryption and to encrypt the filename are used to strengthen cryptographic security. The passphrase is memorized for 2 minutes. As a result, the original file is encrypted by a right click on the file and selecting the appropriate option. The decryption operation is analogous.

4.2. Steganographic embedding of a file or a text into a digital image

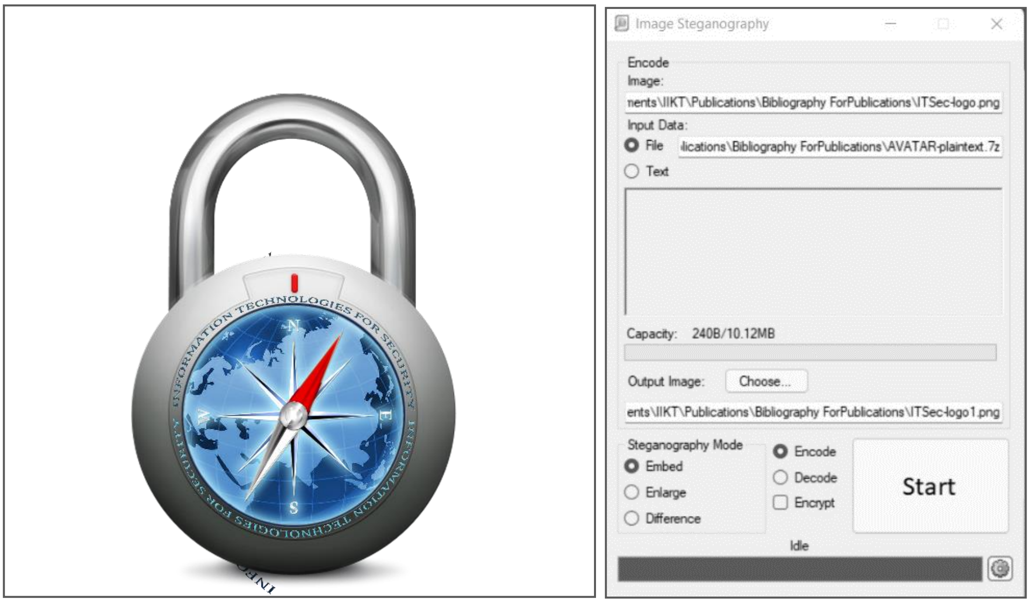
The software Image Steganography 1.5.2.0 used for this part of the empirical research is selected because of its compatibility with encryption software which uses AES algorithm. The encrypted file **AVATAR_plaintext.7z** is embedded inside of the digital image **ITSec-logo.png**. The raster file format PNG (Portable Network Graphics) supports transparent background.

The decoding is realized by using the option ***Output Text*** when the radio button ***Decode*** is on. The output text is: **AVATAR STEGANOGRAPHY**. As a result, the software generates a text in the same field **(AVATAR-plaintext.7z>7z??')** and a notification confirming that the operation has been completed successfully.

4.3. Assessment and analysis of the experimental results.

The author investigates a total of three products to perform the present experimental study. Based on this it can be concluded that the successful implementation of steganographic embedding depends on meeting the following criteria:

- ***compatibility of the steganographic and cryptographic software used is required*** – it is expressed in the use and support of the same cryptographic algorithms.
- ***a steganographic software should support the same compression that is used during the first step of the complex algorithm*** – for example some of them do not support 7z.



Encode
Image: nents\IIKT\Publications\Bibliography ForPublications\ITSec-logo.png
Input Data:
● File ications\Bibliography ForPublications\AVATAR-plaintext.7z
○ Text
Capacity: 240B/10.12MB
Output Image: ents\IIKT\Publications\Bibliography ForPublications\ITSec-logo1.png
Steganography Mode
● Embed
○ Enlarge
○ Difference
● Encode
○ Decode
□ Encrypt
Idle

Fig. 4. Steganographic embedding of an encrypted file into a raster image.

5. CONCLUSION

In conclusion it can be said that computer graphics has proven to play a key role in the process of information protection by advanced steganographic techniques. Besides, the considered cryptographic and compression algorithms (the Vigenere cipher, XOR and etc.) should be combined in order to improve the efficiency in building cybersecurity.

eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii

DOI: https://doi.org/10.33919/YTelecomm.22.9.3

The present research can be continued by extending the study in the direction of steganographic techniques like LSB (Least Significant Bit), MSB (Most Significant Bit) or BPCS (Bit-Plane Complexity Segmentation steganography) through simulations of artificial neural networks for recognition of steganographic images using the Backpropagation algorithm which aims to train neural networks by calculating the error during the recognition process. Such research can contribute to strengthening cybersecurity in term of steganalysis because *"machine learning is used in cybersecurity for both security and criminal activities, incl. and for cyberattacks targeting machine-learning models" [15]*. As a cybersecurity solution this method can be useful for detecting various types of cyber threats, as well as *"to provide practical security standards"[16]*.

REFERENCES:

[1] DANIEL, Brett. What Is AES Encryption? [The Definitive Q&A Guide]. *Trenton Systems* [online]. 31 March 2021 [viewed 20 February 2022]. Available from: https://www.trentonsystems.com/blog/aes-encryption-your-faqs-answered

[2] JASSIM, Nassif K. Hybrid cryptography and steganography method to embed encrypted text message within image. *Journal of Physics: Conference Series* [online]. 2019, vol. 1339, № 012061 [viewed 20 January 2023]. eISSN 1742-6596. Available from: https://doi.org/10.1088/1742-6596/1339/1/012061.

[3] THAYANANTHAN, Vijey. Combining RSA and Vigenère Cipher algorithm to Encrypt and Decrypt Data, CS741 - Applied Cryptography. *Studocu* [online]. Technical University of Mombasa, 2019 [viewed 20 January 2023]. Available from: https://www.studocu.com/row/document/technical-university-of-mombasa/bachelor-of-science-mathematics-and-computer-science/rsavigenere-combining-rsa-and-vigenere-cryptographic-algorithms-to-encrypt-and-decrypt-data/7758083

[4] SARKAR, Subhasish. How much do you know about the Vigenère cipher? *IBM Z Security* [online]. 2020 [viewed 20 January 2023]. Available from: https://community.ibm.com/community/user/ibmz-and-linuxone/blogs/subhasish-sarkar1/2020/07/17/how-much-do-you-know-about-the-vigenere-cipher

[5] NERI, Daniel, Ariel M. SISON, and Ruji P. MEDINA. Performance Analysis of the Modified Vigenere Algorithm to Secure Data. In: *Proceedings of the 9th International Workshop on Computer Science and Engineering (WCSE 2019 SUMMER)*. Hong Kong, 2019, pp. 789-794. ISBN 978-981-14-1684-2.

[6] SUBANDI, Amin et al. Three-Pass Protocol Implementation in Vigenere Cipher Classic Cryptography Algorithm with Keystream Generator Modification. *Advances in Science, Technology and Engineering Systems Journal* [online]. 2017, vol. 5(2), pp. 1-5 [viewed 20 January 2023]. ISSN 2415-6698. Available from: DOI:10.25046/aj020501

[7] ASCII Conversion Chart. *Technical Resources* [online]. [viewed 20 January 2023]. Available from: https://web.alfredstate.edu/faculty/weimandn/miscellaneous/ascii/ascii_index.html

[8] XOR Gate & XNOR Gates: Truth Table, Symbol & Boolean Expression. *Electrical 4U* [online]. 11 October 2020 [viewed 20 January 2023]. Available from: https://www.electrical4u.com/exclusive-or-gate/

[9] What is the difference between Encryption and Compression? What order should they be done in? *Encryption Consulting* [online]. [viewed 20 January 2023]. Available from: https://www.encryptionconsulting.com/education-center/encryption-and-compression/

[10] ZELENSKI, Julie, Keith SCHWARZ, and Marty STEPP. *Huffman Encoding and Data Compression* [online]. [viewed 20 January 2023]. Stanford University and Marty Stepp, licensed under Creative Commons Attribution 2.5 License. Available from:

https://web.stanford.edu/class/archive/cs/cs106x/cs106x.1192/resources/minibrowser2/huffman-encoding-supplement.pdf

[11] CONRAD, Eric, Seth MISENAR and Joshua FELDMAN. Domain 5: Cryptography. In: *CISSP Study Guide* [online]. Second Edition. Amsterdam [u.a.]: Elsevier Inc, 2012, pp. 169-211 [viewed 20 January 2023]. ISBN 978-1-59749-961-3. Available from: https://doi.org/10.1016/B978-1-59749-961-3.00005-4.

[12] SHENE, C. K. *Introduction to Computing with Geometry Notes* [online]. Michigan Technology University, 2014 [viewed 20 January 2023]. Available from: https://pages.mtu.edu/~shene/COURSES/cs3621/NOTES

[13] SALOMON, David. *Curves and Surfaces for Computer Graphics* [online]. New York: Springer, 2005 [viewed 20 January 2023]. ISBN 978-0-387-24196-8. SpringerLink. Available from: https://doi.org/10.1007/0-387-28452-4_3

[14] ANDERSON, Scott D. Affine Transformations Computer Graphics. *Wellesley College* [online]. [viewed 20 January 2023]. Available from: https://cs.wellesley.edu/~cs307/readings-s21/math/04-affine-math.pdf

[15] КЪДРЕВ, Васил и Росен ПАСАРЕЛСКИ. Приложение на подходи на изкуствен интелект и машинно обучение в киберсигурността. *Годишник Телекомуникации 2021* [онлайн]. София: НБУ, 2021, (8), с. 53-64 [прегледан 20 Януари 2023]. eISSN 2534-854X. Достъпен на: https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii-broeve/godishnik-telekomunikacii-2021-g-tom-8 [KADREV, Vasil i Rosen PASARELSKI. Prilozhenie na podhodi na izkustven intelekt i mashinno obuchenie v kibersigurnostta. *Godishnik Telekomunikatsii 2021* [onlayn]. Sofia: NBU, 2021, (8), s. 53-64 [pregleden 20 Yanuari 2023]. eISSN 2534-854X. Dostapen na: https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii-broeve/godishnik-telekomunikacii-2021-g-tom-8]

[16] СИМЕОНОВА, Цветелина и Васил КЪДРЕВ. Развитие на изкуствения интелект и неговото приложение в телекомуникационните мрежи и услуги. *Сборник доклади от Научна конференция с международно участие на НВУ „В. Левски", В. Търново, 27-28.05.2021*. Велико Търново: ИК на НВУ „Васил Левски, 2021, с. 2376-2386. ISSN 2367-7481. [SIMEONOVA, Tsvetelina i Vasil KADREV. Razvitie na izkustvenia intelekt i negovoto prilozhenie v telekomunikatsionnite mrezhi i uslugi. *Sbornik dokladi ot Nauchna konferentsia s mezhdunarodno uchastie na NVU „V. Levski", V. Tarnovo, 27-28.05.2021*. Veliko Tarnovo: IK na NVU „Vasil Levski, 2021, s. 2376- 2386. ISSN 2367-7481.]

Contacts:
Chief Assistant, Dr. Yoana Atanasova Ivanova, New Bulgarian University, Department Telecommunications, Sofia, 21 Montevideo St., e-mail: yivanova@nbu.bg

Дата на постъпване на ръкописа (Date of receipt of the manuscript): 10.04.2022
Дата на приемане за публикуване (Date of adoption for pubication): 30.09.2022