



A Crypto-Stegano Hybrid Application on Spatial Domain

Hüseyin Bilal MACİT*

Burdur Mehmet Akif Ersoy University, Bucak ZTYO, Department of Information Systems and Technologies, Burdur, Turkey

Keywords:

*Vigenère table,
Vigenère cipher,
Steganography,
Avalanche effect*

Abstract

The need for data security in communication is increasing with the developing technology. The best way to ensure data security is cryptography. Humanity has proposed many cryptography methods for hundreds of years. Today, there are complex cryptography algorithms, which are quite secure but require high processing power. Cryptography techniques used in the past are less secure but require less processing power. This article proposes an extended version of the Vigenère cipher, which is an ancient encryption method. Extended Vigenère cipher is able to encrypt upper and lower case letters, numeric characters, and punctuation marks. In addition, the method can use upper and lower case letters, numeric characters and punctuation marks as encryption key, and there is no key length limit. The cipher text generated with the extended Vigenère cipher is also hidden in an image to keep it safe in the transmission medium. Hiding is performed with LSB steganography, which is another data security method. Thus, both the readability and detectability of confidential data are reduced. The cryptological security of the proposed method is measured by the Avalanche effect. Steganographic safety is evaluated with SSIM and PSNR measurements. A user graphical interface has been developed and the maximum payload of the carrier image is measured before encryption. Proposed method applied on some test images with different specifications. 1 bit key modification avalanche effect results of proposed method with random plain texts between 1000-10000 characters with a key length of 8 and 16 characters is close to 50%. Also, SSIM value calculated over 0.99 each time while maximum steganographic payload of the test images reached.

*e-posta: hbmact@mehmetakif.edu.tr

Bu makaleye atıf yapmak için:

Hüseyin Bilal MACİT, "A Crypto-Stegano Hybrid Application on Spatial Domain", Bayburt Üniversitesi Fen Bilimleri Dergisi, C. 5, s 2, ss. 154-164

How to cite this article:

Hüseyin Bilal MACİT, "A Crypto-Stegano Hybrid Application on Spatial Domain", Bayburt University Journal of Science, vol. 5, no 2, pp. 154-164

1 INTRODUCTION

Cryptography is a term formed by the combination of the ancient Greek words *kryptós* (κρυπτός) meaning secret and *graphein* (γράφειν) meaning writing [1]. Cryptography is the art of producing confidential messages [2]. The main purpose of cryptography is to provide a secure exchange of information between two parties without interference by external factors [3]. Cryptography aims to transform information into a format that is incomprehensible to anyone but the sender and receiver. Cryptography uses encryption and a decryption algorithm. The sender encrypts the information and sends it. The receiver must know the decryption method in order to be able to read the information received correctly [4]. If the third gets information about the decryption algorithm, the cryptography algorithm must be changed. Since it is difficult to develop a new algorithm each time, cryptography uses keys as well as algorithms. Thus, the sender and receiver can continue to use the same algorithm by only changing the key value [5]. The security of encrypted data depends on the strength of the cryptographic algorithm and the confidentiality of the key [6]. The main purposes of cryptography are authentication which is the sender to prove his identity to the receiver, confidentiality which guarantees that the transmitted information reaches only the authorized receiver, access control which prevents unauthorized access to information and non-repudiation which proves that the incoming message comes only from the sender [2, 3]. In cryptography, a message created by the sender and not yet encrypted is called plain text. The encryption algorithm converts the plain text to unreadable cipher text using a key value. Figure 1 shows a simple cryptology process of a message M where E stands for encryption and D is for decryption.

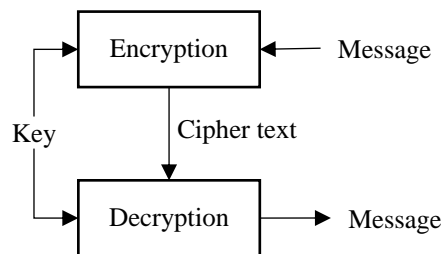


Figure 1. Common method of cryptology [7]

The cipher text is transmitted over a public transmission channel. So, it can be intercepted by third parties or even read if the decryption algorithm and key are known. We can hide the presence of cipher text in the transmission channel using steganography. The term steganography is a combination of the ancient Greek words *steganós* (στεγανός) meaning covered and *graphein* (γράφειν) meaning writing. Steganography sends a message by hiding it inside a cover object. Malicious third parties do not doubt it when they encounter the cover object [8]. Steganography techniques are used in many areas such as copyright protection, confidential information protection, and confidential communication [8].

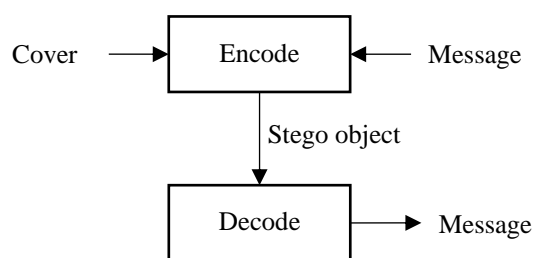


Figure 2. Common method of steganography

We can protect the message by encrypting it, but we cannot hide the existence of the message during transmission. Steganography protects the message by hiding it without attracting suspicion. By using steganography and cryptology methods together, we can both hide the existence of the message and make it difficult to read it even if it is intercepted. In this study, we proposed and implemented a hybrid data security method by using a combination of Vigenère encryption, which is a cryptology method, and the steganographic method in the spatial domain.

This paper is divided into the following sections. In Section 2, we explained some articles and methods carried out in the literature before. In section 3, we mentioned the history and algorithm of the Vigenère cipher. We listed some example results of the improved Vigenère cipher to show its advantages. We also mentioned the steganography method we used and the chosen color space in this section. In the 4th section, we showed the graphical user interface (GUI). We explained some mathematical methods we used to measure the reliability of

the proposed method. Then, we analyzed the performance of the proposed method by using plaintexts of different lengths and covering images with different features. Finally, we evaluated obtained results in Chapter 5.

2 RELATED WORK

Mandal and Deepti [6] proposed a new method to obtain a new ciphertext, which is applied in the Vigenère table by selecting the equivalent fixed-length plaintext and a key. In their study, the text is sent twice encrypted and decrypted by performing the reverse operation at the receiver. The proposed method is compared with AES, Blowfish, and RC5 algorithms. Considering the possible combinations, it is predicted that the proposed 256-bit encryption method will take 4×10^8 years to crack. Saraswat et al. [1] expanded the Vigenère table to include numerical data in their work. So, they also encrypted the numbers using this technique. They combined the encryption process of the Vigenère and Caesar cipher to obtain the ciphertext from the separately supplied plaintext and key. Gautam et al. [3] combined the coding method of Vigenère and modified Caesar cipher to obtain the ciphertext from the given plaintext and key. Soofi et al. [9] proposed an improved version of the traditional Vigenère cipher that eliminates the possibility of a Kaisiski and Friedman attack. The proposed technique also provides better security against cryptanalysis and model prediction. Nahar and Chakraborty [5] expanded the Vigenère table to include all possible upper and lower-case characters, mathematical symbols, and numbers. They used the proposed Vigenère table for cipher text generation. However, they did not use all these characters as keywords. Senthil et al. [Senthil] strengthened Ceaser cipher method with a set of mathematical tools. The aim of the study is to preserve the basic philosophy of Ceaser cipher and make it more resistant to cryptanalysis. As a result of their studies, they stated that the proposed method can be used with Vigenère encryption. Konyar and Solak [11] proposed a new method based on Vigenère in video steganography. As a result of their studies, it is seen that the method they proposed is above 65 dB Peak Signal to Noise Ratio (PSNR) value and 0.99 Structured Similarity Index (SSIM) value at 20 kbit data capacity. In addition, when there is no significant loss in SSIM value, approximately 55 dB and 50 dB PSNR values are reached at 200 kbit and 500 kbit data capacities, respectively. Laskar and Hemachandran [8] proposed a data embedding approach with a combination of steganography and cryptography. In their work, a message is first encrypted using the transposition encryption method, and then the encrypted message is embedded into an image using the LSB insertion method. To demonstrate the effectiveness of the method, they calculated Mean Square Error (MSE) and PSNR and performed comparative analysis. They also analyzed the data hiding technique using image performance parameters such as entropy, mean and standard deviation. Hammad et al. [12] proposed a combination of Vigenère and Ceaser Cipher methods. The ciphertext obtained in the proposed method is converted to the names of chemical elements in the periodic table. Also, they added a scroll trick in the method. The ciphertext obtained after all these processes is embedded in an image file with the LSB steganography method. Voleti et al. [13] embedded Vigenère cipher-encrypted text into image files using LSB steganography. LSB steganography works on images in bitmap format. The most important feature of this study is that it can apply the LSB steganography technique to image files of all formats without any transformation. Sermeno et al. [14] used a hybrid approach of the Vigenère encryption system to encrypt and decrypt data. This approach is integrated with the learning management system using matrix manipulation and Base94 coding scheme. The experimental result of the study shows a significantly higher avalanche effect compared to the original Vigenère encryption system.

3 MATERIAL AND METHOD

Basic cryptography algorithms are divided into two classes, monoalphabetic and polyalphabetic. The monoalphabetic algorithm creates cipher text by substitution of each character in plain text with another character. In this method, cipher text can easily be decrypted by frequency analysis. Encryption with the Polybius square is an example of this approach. The polyalphabetic algorithm, on the other hand, can substitute a character with a different one each time. Thus, cipher text cannot be easily encrypted by frequency analysis. In this paper, we implemented a modified Vigenère encryption as the cryptography method. The Vigenère Cipher is a polyalphabetic encryption scheme invented by Blaise De Vigenère in the 16th century [6]. It uses the Vigenère table (Figure 3), in which the 26-character Latin alphabet is written in 26 lines, one shifted to the left each time [10].

Vigenère Cipher uses the same key for both encryption and decryption. Therefore, it is a symmetric algorithm [3]. The key must be the same length as the message. If the key is shorter, it is repeated enough to make it the same size as the message. We generate each character of cipher text with the intersection of each character of generated key and each character of the plain text in the table. Let, the message be $M = \text{''HBMACIT''}$ and Key $K = \text{''ABC''}$. In this case, the cipher text is formed as in Table 1.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X

Figure 3. 26x26 Vigenère table

Table 1. Sample Vigenère encryption

Plain text	H	B	M	A	C	I	T
Key	A	B	C	A	B	C	A
Cipher text	H	C	O	A	D	K	T

Let, m is length of message, $P_0 \dots P_m$ is the plain text, $C_0 \dots C_m$ is the ciphertext and $K_0 \dots K_m$ is the key. Equation 1 defines the encryption and Equation 2 defines the decryption process:

$$C_m = (P_m + K_m) \bmod(26) \tag{1}$$

$$P_m = (C_m + K_m) \bmod(26) \tag{2}$$

The 26-character Vigenère square contains only capital letters. In this paper, we generated a 95-character Vigenère square including uppercase, lowercase, numbers and punctuation marks. First row of it includes {space !” # \$ % & '()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMN OPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~

We can encrypt many ASCII characters with this improved Vigenère table. We can also generate more complex keys including uppercase, lowercase, numbers, and punctuation marks. For example, we can generate a 3-character key in $26 \times 26 \times 26 = 17576$ different ways in a 26-character Vigenère table, while we can generate it in $95 \times 95 \times 95 = 857375$ different ways in an improved 95-character Vigenère table. Encryption operations with different variations are shown in Table 2.

Table 2. Samples results of improved Vigenère table

	Plain text	Key	Cipher text
Same plain text with different keys	hbmait	0.hbm%A?	xpVDQn%
		9a-3%"?M	"Dzthk.
		aa1.%?_@	JD~oh)V
Similar plain texts with same key	This is an article		dvRVmn\$.JQmf##RFZj
	This is a new article	0.hbm%A?	dvRVmn\$.Jb\j(.JUBnszN
	It is a new article		Y#hLa%q.WHe%q!]LQqu

The larger Vigenère table provides more secure encryption. However, due to the developing processor speeds, Vigenère encryption can be broken by using various methods such as Kasiski and Friedman tests [9]. It is not possible for a message to be read maliciously without being intercepted in the communication medium. In this

paper, we proposed a steganographic method to securely transmit the Vigenère encrypted message to the receiver. Images, audio files and videos are used as cover objects for steganography, but the most popular cover object is images [15]. An image is a combination of dots called pixels arranged in a grid pattern, each numerically expressing different light intensity. There are three types of images according to the number of colors; black and white (binary), monochrome and color. The maximum amount of data that can be hidden in an image is called the payload. A color image may contain more confidential data because it contains more than one color scheme. So it has more payload. The most commonly used color schemes to express color images are color-based Red Green Blue (RGB), tone-based Hue Saturation Value (HSV), and luminance-chrominance-based (YCbCr) [15].

An important goal in steganography is that the change in the encoded image is not easily detectable by the human visual system (HVS) and software. The HVS easily detects a change in brightness in an image, but cannot detect minor color changes. Using this weakness of HVS, we aimed to embed the cipher text, which we created with Vigenère encryption, into the chrominance channels of the cover image. We used the "peppers" image shown in Figure 4 as a test image while implementing the proposed method. Let, I is an RGB image with m rows and n columns;

$$I(m, n) = \{x_{i,j} | 1 \leq i \leq m, 1 \leq j \leq n\} \tag{3}$$

Each $x_{i,j}$ represents a pixel of I . To convert I to YCbCr color scheme;

$$\begin{pmatrix} Y \\ Cb \\ Cr \end{pmatrix} = \begin{pmatrix} 0.299 & 0.587 & 0.114 \\ -0.169 & -0.331 & 0.500 \\ 0.500 & -0.419 & -0.081 \end{pmatrix} \begin{pmatrix} R \\ G \\ B \end{pmatrix} + \begin{pmatrix} 0 \\ 128 \\ 128 \end{pmatrix} \tag{4}$$

Y , Cb and Cr matrices are obtained. Y represents the luminance, Cb represents Blue-chrominance and Cr represents Red-chrominance. Figure 4 shows plotted Y , Cb and Cr matrices of test image.

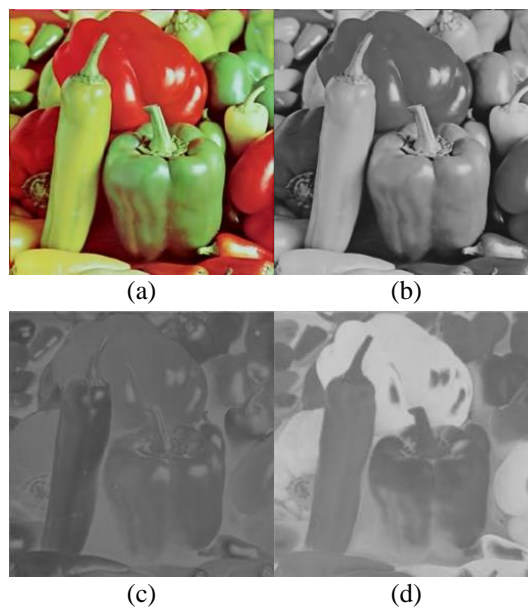


Figure 4. (a) Test image (b) Y channel (c) Cb channel (d) Cr channel

In a 24-bit color image, Cb and Cr chrominance channels each carry 8 bits of data. Let $p_{i,j}$ be the pixel in the i .row j .column of a channel, the binary expression of this pixel is shown in Figure 5.

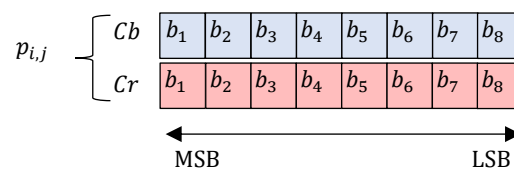


Figure 5. Binary representation of chrominance channels

Steganographic methods are examined in two classes as spatial and frequency domain. Methods in the frequency domain process the image as a signal function and use wavelet transform methods. These methods hide confidential data in a robust but detectable way. Spatial domain methods are related to insignificant bits of the pixel values. The value range for the 8-bit $p_{i,j}$ pixel is $0 < p_{i,j} < 255$. The most significant bit here is b_1 , because changing b_1 from 0 to 1 or 1 to 0 decreases or increases the pixel value by 128. The least significant bit is b_8 , because changing b_8 from 0 to 1 or 1 to 0 only changes the pixel value by 1. In this paper, we transformed b_6, b_7 and b_8 of each pixel to hide the cipher text. Here, the maximum possible change of value of a pixel in the chrominance scheme is $\frac{2^3}{2^8} = 3.125\%$.

We add *NULL* as the terminating character to the end of the l -length cipher text generated with Vigenère encryption. In this case, the new plain text becomes $P_{m+1} = P_m + \text{NULL}$ and $l = l + 1$. Next, we defined a binary string A , where each character of cipher text is represented by 9 bits.

$$A = \{a_1, a_2, \dots, a_n\}, a_k \in \{0,1\}, n = 9xl \quad (5)$$

The maximum payload of cover image I is calculated as $\mu_I = mxnx6$. A page of text written in a computer program without paragraph spacing contains an average of 4000 characters. In this case, for example, we can embed 393 pages of text in a 512x512 pixel color image. To embed the binary string A in I , it must be $\mu_I > n$. We perform a horizontal scan on I until all A_k 's are embedded. As long as $k < n$ for $p_{i,j}$ each step we perform Equation 6 and Equation 7;

$$Cb_{i,j}(b_6, b_7, b_8) = A(k++) \quad (6)$$

$$Cr_{i,j}(b_6, b_7, b_8) = A(k++) \quad (7)$$

When $k = n$, we terminate the scan. Then, we combine resulting modified Cb and Cr matrices with pure Y matrix to generate a stego S image. We can now send S over a unsecure communication channel to the receiver. Figure 6 shows 11517-character cipher text embedded text image with the proposed method.



Figure 6. (a) Test image (b) Stego image

When the receiver acquires the S image, it generates Y, Cb and Cr channels in the same way as the sender. The receiver knows that there is some hidden data on the Cb and Cr channels, but does not know the size of the data and in which pixels it is located. To read the binary array A , the embedding is done in reverse, which is named extracting. We perform horizontal scanning on S :

$$A_{k,k+1,k+2,\dots} = Cb_{i,j}(b_6, b_7, b_8), Cr_{i,j}(b_6, b_7, b_8) \quad (8)$$

When the length of A (l) is equal to 9, the binary array A now represents a character of the cipher text. To create the cipher text C_m ;

$$C_{i+1} = [C_i A_{k,k+1,\dots,k+8}] \quad (9)$$

We clearly know that the sender terminated the A array with the *NULL* character. If $C_i = \text{NULL}$, cipher text C_m is already created. Then, we terminate the extraction process. If the receiver computer does not know the Key, it cannot decrypt the cipher text. If the key is known, the cipher text is decrypted to plain text by applying the procedure in Equation 2.

4 RESULTS

We coded the proposed algorithm using the Matlab programming language and developed two GUIs for the transmitter (Figure 7) and receiver (Figure 8) side.

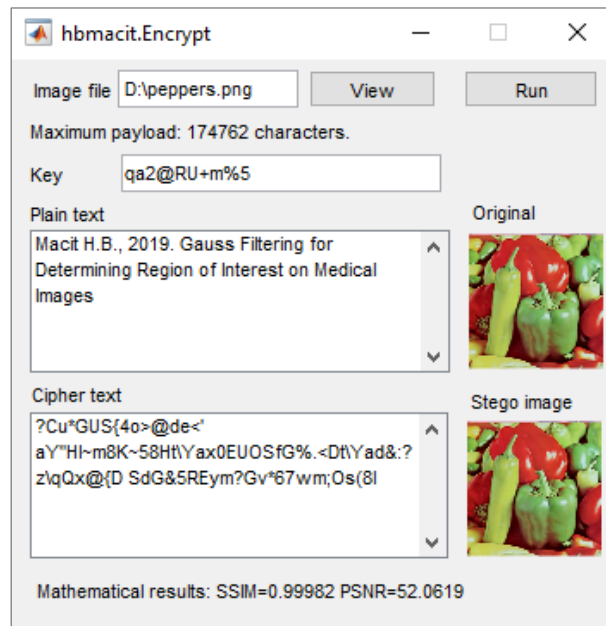


Figure 7. Transmitter side GUI

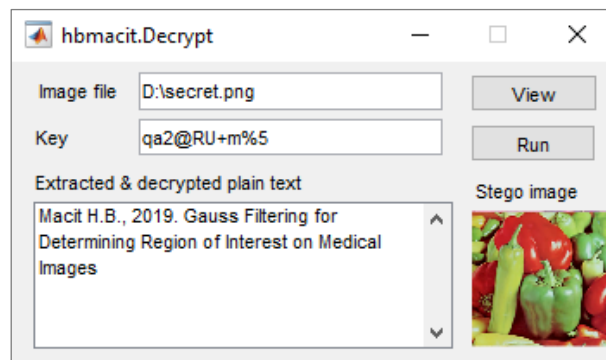


Figure 8. Receiver side GUI

The proposed algorithm combines steganography and cryptology methods. Therefore, the success of the algorithm should be evaluated from both aspects. The success of a steganography algorithm is measured by payload, security, and imperceptibility. With the proposed method, an average of 3,000 pages of text can be embedded in a 2 megapixels resolution image. The transmitter-side GUI shows the maximum payload information when the cover image is uploaded. Image security is the ability to read confidential data correctly after various attacks on the image. However, steganography methods using text as confidential data are weak in terms of security. In other words, the image loses its confidential data in modifications such as cropping, geometric changes, and copy-paste. The imperceptibility of a steganographic image is measured by how far the stego image is from the cover image. If the image is considered as a signal, the alteration in the cover image can be calculated by the distance between the two signals. For this, we calculated PSNR and SSIM of I and S . PSNR calculates the noise between two signals using the MSE. Let x_i and y_i be samples of I and S , respectively;

$$MSE(I, S) = \frac{1}{N} \sum_{i=1}^N (x_i - y_i)^2 \quad (10)$$

L is the peak value of a signal. Here, the peak value is the maximum numerical value of a pixel.

$$PSNR = 10 \log_{10} \frac{L^2}{MSE} = 10 \log_{10} \frac{255^2}{MSE} \quad (11)$$

If two signals are the same, $PSNR = \infty$ [16]. We expect $PSNR > 40$ for an image steganography method to be imperceptible. However, PSNR is a mathematical approach and is not directly related to HVS. We calculated SSIM to get results closer to HVS. SSIM calculates the similarity between I and S in Equation 12.

$$SSIM(I, S) = \frac{(2\mu_I\mu_S + (0.01xL)^2)(2\sigma_{IS} + (0.03xL)^2)}{(\mu_I^2 + \mu_S^2 + (0.01xL)^2)(\sigma_I^2 + \sigma_S^2 + (0.03xL)^2)} \quad (12)$$

Here, μ_I is the mean of I , μ_S is the mean of S , σ_{IS} the covariance of I and S , σ_I^2 is the variance of I , and σ_S^2 is the variance of S . If I and S are the same, the SSIM value is calculated as 1. As the distance between images increases, the SSIM approaches 0. The transmitter side GUI (Figure 7) displays the PSNR and SSIM values of cover and stego image. We embedded cipher texts with length between 64 characters and 131072 characters in the test image and obtained PSNR and SSIM values. As the number of characters increased within the specified range, the PSNR value decreased from 52.0893dB to 34.8527dB and SSIM value decreased from 0,9998 to 0,9911. Figure 9 shows the relationship between character count and PSNR and Figure 10 shows the relationship between character count and SSIM measure.

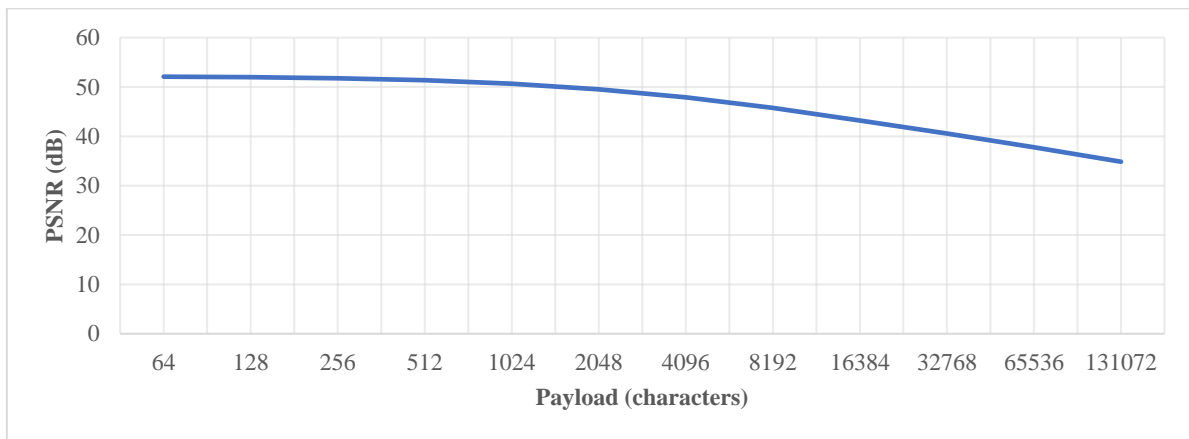


Figure 9. Payload-PSNR graph

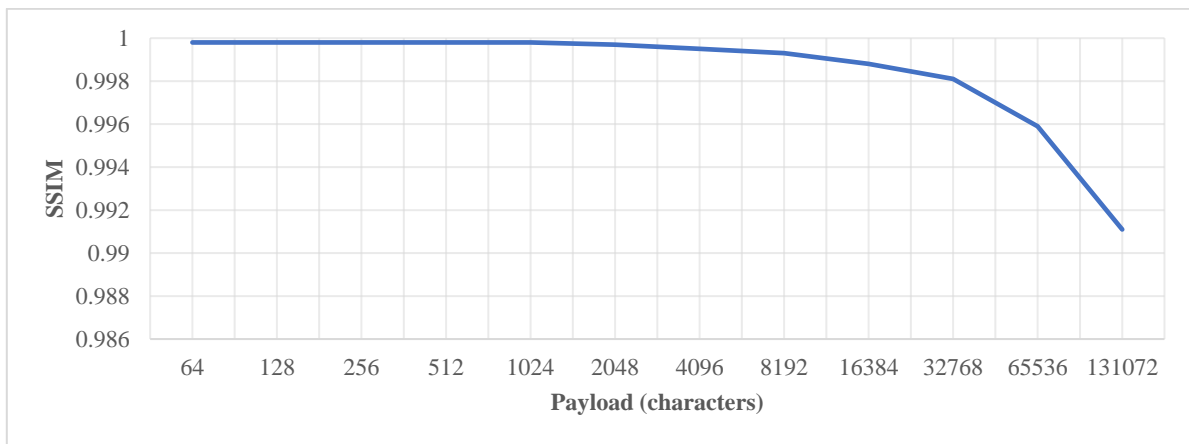



Figure 10. Payload-SSIM graph

When we reach half of the maximum payload value, the PSNR value is measured below 40. So, we can say that high payload values can be noticeable by a special computer algorithm. However, SSIM is a closer measurement to HVS. It is clearly seen in the figure that even if the number of characters approaches the maximum payload, the measured SSIM value shows that it is not possible to distinguish the cover image and the stego image with HVS.

To discuss the steganographic performance of the proposed method, we also encrypted 128 characters and 1024 characters of plaintext with 8bit and 16bit keys and then, we embedded these obtained ciphertxts in 4 different test images. Table 3 shows the characteristic specifications, SSIM and PSNR results of these processes.

Table 3. SSIM and PSNR results of test images

Image						
Name	Peppers	Lena	Baboon	Grass		
Resolution (pixels)	512x512	512x512	256x256	1024x1024		
Size	328KB	101KB	202KB	506KB		
Maximum payload (characters)	174762	174762	43690	699050		
Plaint text length (characters)	Key length (characters)	SSIM	0.9998	0.9998	0.9998	0.9998
		PSNR(dB)	51.9806	51.8723	51.3286	52.0411
128	8	SSIM	0.9998	0.9998	0.9998	0.9998
		PSNR(dB)	51.9859	51.8601	51.2972	52.0355
128	16	SSIM	0.9998	0.9998	0.9996	0.9998
		PSNR(dB)	50.6534	50.6201	47.8966	51.6825
1024	8	SSIM	0.9998	0.9998	0.9996	0.9998
		PSNR(dB)	50.6515	50.6133	47.8672	51.6681
1024	16	SSIM	0.9998	0.9998	0.9996	0.9998
		PSNR(dB)	50.6515	50.6133	47.8672	51.6681

The success of a cryptography technique depends on whether it is decrypted by a cryptanalyst [3]. Mono-alphabetic encryption methods are vulnerable to frequency analysis as each character is constantly substituted by the same character. Frequency analysis pre-calculates the probability of occurrence of each letter in an average text and tries to replace substitution characters. In this case, plain text can be generated by calculating the index of coincidence (Equation 13) [17].

$$ioc = \frac{\sum_A^Z f_i(f_i-1)}{l(l-1)} = \frac{\sum_A^Z f_i(f_i-1)}{95 \times 94} \quad (13)$$

Where f_i is the frequency of i .character. Vigenère cipher is resistant to index of coincidence and frequency analysis because it can substitute a character with different characters each time depending to the length of key. But if the cryptanalyst guesses the key length, the cipher text can be thought of as nested Caesar ciphers.

A good way to evaluate the performance of the Poly-alphabetic encryption method is the Avalanche Effect measurement (Equation 14). The Avalanche Effect predicts that a small change in the key or plain text will result in a significant change in the cipher text. Avalanche Effect > 50% is expected for a very good encryption algorithm.

$$Avalanche\ Effect = \frac{modified\ bits\ of\ cipher\ text}{total\ bits\ of\ cipher\ text} \quad (14)$$

Avalanche effect results of the proposed method with some random parameters are shown in Table 4.

Table 4. Avalanche effect results of proposed cipher

Plain text length (characters)	Key length (characters)	Avalanche effect (%)		Time (sec)
		1-bit modification on key	1-bit modification on plain text	
1279	8	47.7972	0.0459	0.514
	16	39.8027	0.0119	0.506
3839	8	48.5269	0.0038	1.646
	16	45.8002	0.0040	1.821
11517	8	48.4252	0.0013	2.346
	16	48.0103	0.0053	2.302

5 CONCLUSION

The original Vigenère table includes 26x26 characters and contains only capital letters. Vigenère encryption is not robust to frequency analysis. The proposed Vigenère table consists of 95 characters and it includes uppercase, lowercase, numbers and punctuation marks. If a key of sufficient length is used, it is highly resistant to frequency attacks. We also combined it with steganography to make it more secure. We embedded cipher text to an image in the spatial domain. Embedding takes place in chrominance channels, where HVS is most insensitive. The proposed method does not require high processing power. We inform the user in advance of the maximum payload of an image by the GUI. According to the mathematical results we obtained, the length of the ciphertext should not exceed half of the maximum payload value for the best imperceptibility. The user has a chance to choose a better cover image from the beginning using the maximum payload value. In future studies, Turkish character support can be added to the Vigenère table.

Author Contributions

Hüseyin Bilal Macit: Conceptualization, Methodology, Software, Validation, Formal analysis, Investigation, Resources, Data Curation, Writing - Original Draft, Writing - Review & Editing, Visualization, Supervision, Project administration, Funding acquisition

Conflict of interest

No conflict of interest was declared by the authors.

References

- [1] A. Saraswat, C. Khatri, Sudhakar, P. Thakral, and P. Biswas, "An Extended Hybridization of Vigenère and Caesar Cipher Techniques for Secure Communication," *Procedia Computer Science*, Vol. 92, pp. 355 – 360, 2016.
- [2] K.I. Rahmani, N.Wadhwa and V. Malhotra, "Alpha-Qwerty Cipher: An Extended Vigenère Cipher," *Advanced Computing: An International Journal*, Vol. 3, no. 3, pp. 107-118, 2012.
- [3] D. Gautam, C. Agrawal, P. Sharma, M. Mehta and P. Saini, "An Enhanced Cipher Technique Using Vigenère and Modified Caesar Cipher," *2nd International Conference on Trends in Electronics and Informatics*, vol. 1, no. 9, 2018.
- [4] I. Saputra, N.A. Hasibuan, Mesran and R Rahim, "Vigenère Cipher Algorithm with Grayscale Image Key Generator for Secure Text File," *International Journal of Engineering Research & Technology*, vol. 6, no. 1, pp. 266-269, 2017.
- [5] K. Nahar and P. Chakraborty, "A Modified Version of Vigenère Cipher using 95 × 95 Table," *International Journal of Engineering and Advanced Technology*, vol. 9, no. 5, pp. 1144-1148, 2020.
- [6] S.K. Mandal and A.R. Deepti, "A Cryptosystem Based On Vigenère Cipher By Using Multilevel Encryption Scheme," *International Journal of Computer Science and Information Technologies*, vol. 7, no. 4, pp. 2096-2099, 2016.
- [7] H.B. Macit, A. Koyun and M.E. Yüksel, "Embedding Data Crypted With Extended Shifting Polybius Square Supporting Turkish Character Set," *BEU Fen Bilimleri Dergisi*, vol. 8, no. 1, pp. 234-242, 2019.
- [8] S.A. Laskar and K. Hemachandran, "High capacity data hiding using LSB steganography and encryption," *International Journal of Database Management Systems*, vol. 4, no. 6, 2012.
- [9] A.A. Soofi, I. Riaz and U. Rasheed, "An Enhanced Vigenere Cipher For Data Security," *International Journal of Scientific & Technology*, vol. 5, no. 3, pp. 141-145, 2016.
- [10] K. Senthil, K. Prasanthi and R. Rajaram, "A Modern Avatar of Julius Caesar and Vigenère Cipher," *Proceedings of IEEE International Conference on Computational Intelligence and Computing Research*, 2013.
- [11] M.Z. Konyar and S. Solak, "Efficient data hiding method for videos based on adaptive inverted LSB332 and secure frame selection with enhanced Vigenere cipher," *Journal of Information Security and Applications*, vol. 63, 2021.
- [12] R. Hammad, K.A. Latif, A.Z. Amrullah, H., A. Subki, P. Irfan, M. Zulfikri, L.Z. Azhar, M. Innuddin and K. Marzuki, "Implementation of combined steganography and cryptography Vigenere cipher, caesar cipher and converting periodic tables for securing secret message," *Journal of Physics: Conference Series* 2279, 2022.

- [13] L. Voleti, R.M. Balajee, S.K. Vallepu, K. Bayoju and D. Srinivas, "A Secure Image Steganography Using Improved LSB Technique and Vigenere Cipher Algorithm, " *Proceedings of the International Conference on Artificial Intelligence and Smart Systems*, pp. 1005-1010, 2021.
- [14] J.P. Sermeno, K.A.S. Secugal, N.E. Mistio, "Modified Vigenere cryptosystem: An integrated data encryption module for learning management system," *Convergent Technologies for Innovative Learning Environment and Information Systems*, vol. 18, no. 4, 2021.
- [15] S. Hemalatha, U.D. Acharya and A. Renuka, "Comparison of Secure and High Capacity Color Image Steganography Techniques in RGB and YCbCr Domains," *International Journal of Advanced Information Technology*, vol. 3, no. 3, 2013.
- [16] H.B. Macit and A. Koyun, "A New Imperceptible Steganography Method for Grayscale Images," *Journal of Engineering Sciences and Design*, vol. 8, no. 2, pp. 357-365, 2020.
- [17] B. Henry, "Cipher systems, the protection of communications," London, Northwood Books, 1982.