Research Article

Journal of Electrical Electronics Engineering

Analysis of Cryptography before Steganography Operation by ROC Curves and Confusion Matrices Criteria

A. Hadipour[1*], R. Afifi[2] and H. ShojaeiYas[3]

[1]*Cryptography and coding Department, Isfahan Mathematics House, Isfahan, Iran*

[2]*Mathematics Department Ale-Taha University, Tehran, Iran*

[3]*Malek-Ashtar University of Technology, Tehran, Iran*

***Corresponding author**

A. Hadipour, Cryptography and coding Department, Isfahan Mathematics House, Isfahan, Iran

Submitted: 17 Aug 2022; **Accepted:** 24 Aug 2022; **Published:** 20 Sep 2022

Citation: *Hadipour A*, Afifi R and ShojaeiYas H. (2022). Analysis of Cryptography before Steganography Operation by ROC Curves and Confusion Matrices Criteria. . J Electrical Electron Eng, 1(1), 48-63.*

Abstract

The steganography algorithms based on media type, format and capacity are used for different applications. The use of cryptographic algorithms also depends on the type of application. The challenge that can be investigated is the use of cryptographic algorithms in the steganography process, which must be properly scrutinized due to the special sensitivities of these two technologies. The use of cryptographic algorithms in steganographic systems increases the security of hidden data, but this security level should not make the entropy more visible and did not consider other metric. For this reason, in this paper, two steganographic algorithms for JPEG image and two steganographic algorithms for audio in WAV format are investigated, so that before the steganographic operation, a cryptography algorithm is used to encrypt the message. In the following, after reviewing the steganographic algorithms using several valid steganalysis, the advantages of using and not using these cryptographic algorithms against their disadvantages are reviewed and suggestions about their use in steganography algorithms and systems are presented.

Key Words: Steganography, Cryptography, ROC Curve, Confusion Matrix, Capacity

Introduction

The use of cryptographic algorithms to embedding encrypt messages in digital envelopes has always been questioned by many researchers in this field. The process of encrypting a message before it is used for steganography purposes is used in two ways: the symmetric key and the public-private key. For symmetric algorithms, a symmetric key is defined, and for asymmetric algorithms, public-private key is defined. The use of each of cryptography depends on the type of usage.

The use of cryptography in steganography is a topic that has not been seriously addressed, and comparisons between the two sciences have always been made for their applications. In a few papers, the use of cryptography in steganography has been introduced in a very simple and transient way, and the reason for using it has been suggested in order to make the system more secure. While this can have its advantages and disadvantages. For example, proposed a way to implement the steganography algorithm in the cryptographic system in order to hide the data in a medium and provide more security [1]. The media used in this steganographic system is audio and the algorithm used in it for data hiding operations is Least Significant Bit (LSB) method. The encryption and decryption algorithm used in this system will increase the security of the hidden data [2]. Proposed a system that combines cryptography and stenography operations, in which a more powerful and qualified LSB method performs stenographic operations using an audio file as a cover for a confidential message, to ensure security and used to ensure the security of the information sent [3]. Has introduced various types of audio media based steganography methods by presenting its advantages and disadvantages. In this paper, a method with appropriate and powerful revenue in order to hide the unperceivable audio data is presented. This paper claims that audio data hiding techniques can be used for purposes other than hiding or storing undeniable information, manipulating detection, fingerprinting and tracking information.

Provided better security and confidentiality on how to combine both steganography and cryptography. Cryptography algorithms make information incomprehensible to anonymous people so that no aggressor can interpret the plaintext sent. However, stegano-

graphic algorithms focus on the concealment existence of the confidential information and are used for this purpose [4].

The steganography process in any digital media, with or without the use of cryptographic algorithms, must be done intelligently, so that its evaluation criteria such as MSE, PSNR, histogram and ROC diagrams and confusion matrices are accepted. The following equations is used to calculate the MSE and PSNR.

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left(I\left(i,j\right)-K\left(i,j\right)\right)^2 \quad (1)$$

$$PSNR = 10\log_{10}\frac{\left(MAX_I^{\,2}\right)}{MSE} = 20\log_{10}\frac{MAX_I}{\sqrt{MSE}} \quad (2)$$

They also use staganalysis algorithms to obtain ROC curves and confusion matrices. Staganalysis algorithms are designed and used to rely on two types based on steganography method and blind. Also, each of them can be implemented and executed based on the type of media and the type of format [5].

In this paper, we have tried to express the author's view on the type of evaluation of steganography algorithms in the use and non-use of cryptographic algorithms. The following are the advantages and disadvantages of using cryptographic algorithms in steganography algorithms, citing the reasons and diagrams of the standard analysis.

Therefore, section 2 will examine how to hide in widely used media. In Section 3, cryptographic algorithms will be examined in two symmetric and asymmetric methods. In Section 4, the advantages and disadvantages of using cryptographic algorithms in steganography will be presented with examples and evaluated by standard evaluators. Section 5 concludes the paper.

Steganography

Data hiding refers to the science of invisible communications. In other words, the hiding of information is the art of hiding information in a media carrier and can enable a security entity to conceal the information in the form of a covering factor, like audio, image and video, hide in the original file without making any significant changes and will be move between the desired point with the utmost care for security. Hiding information in any medium and in any format can be implemented in a variety of ways. Therefore, it is possible to name the methods of inserting in the least significant bit, wavelet transforms and etc. in audio, inserting DCT and AC coefficients and etc. in the image and inserting motion vectors, masking and filtering methods and etc. in the video. Embedding a message in each of these methods has completely different techniques.

So in a word, steganography is a technique for hiding information from an enemy and will create an invisible connection. All steganographic systems consist of a cover medium, so that confidential information is embedded in them. The process of inserting confidential information into a medium will produce a stego environment, and the resulting media will be called a stego media. To hide confidential information, steganography will provide the transmission.

Steganography is the art of hiding confidential messages in a folder with minimal possible auditory and visual changes without leaving a significant trace of the original message.

Cryptography

Cryptography is the art and knowledge of achieving security through message encryption so that the converted data is unreadable, meaning that it will be used to protect user data. Encryption and decryption are the two main functions of cryptography. Encryption is the process of transforming original plaintext (which the original plaintext is readable) into the ciphertext (which the data is unreadable). Where decryption is just opposite process of encryption in which we retrieve the original plaintext from ciphertext. Cryptography is basically used so that unauthorized access can be prevented. There are two types of modern cryptosystems: symmetric cryptography and asymmetric cryptography.

Symmetric Cryptography

One type of encryption is symmetric cryptography, in which only one key (secret key) is shared and the same is used to encrypt/decrypt electronic information. The people communicating through symmetric encryption must exchange the key to be used in the decryption process. The use of new symmetric cryptographic algorithms will follow the same process [6]. This type of encryption is different from asymmetric cryptography, where a key pair, one public and one private, is used to encrypt and decrypt messages. The public key is disclosed to everyone, but each person's private key is unique and completely confidential.

When symmetric encryption algorithms are used, the data will be transformed in a way that is incomprehensible to someone who does not have that secret key and cannot actually decrypt the data. In this type of cryptography, after a message with a specific key is sent to the intended recipient, the operation of the algorithm is reversed and the message is returned to its original and understandable form so that the recipient can read the encrypted message clearly. In this case, the secret key can be made in different ways. These keys are usually created by a stream of numbers or characters by secure random number generators (RNGs) and are used same by the sender and receiver. For example, at the banking-level, symmetric keys should be used for encryption and decryption, and how to generate these keys using RNG is possible, as approved by industry standards such as FIPS 140-2.

There are two types of symmetric cryptographic algorithms. The first, block cipher algorithms, which encrypt a set of bit lengths in electronic data blocks using a special secret key. By encrypting the data, the system keeps the data in its memory, waiting for complete blocks. The second, stream cipher algorithms, in which data is encrypted as a stream of data rather than stored in system's memory. Because symmetric cryptography is an old method of encryption, it is faster and more efficient than asymmetric cryptography and can damage networks due to performance problems in data size and amount and the use of heavy processors.

Because the performance and speed of symmetric encryption (compared to asymmetric) is better and faster, symmetric encryption is generally used to encrypt/decrypt large amounts of data. In order to encrypt a database on a database, the secret key is only available to the database for encryption or decryption.

Some examples used in symmetric cryptography are listed below: (1) Payment application systems, such as bank card transactions, in which PII must be protected in order to prevent fraudulent charges, identity theft or money laundering. (2) Message authentication, when the sender sends a message and claims to be the sender of the same person. (3) Random number generation or hash functions.

Key management of symmetric cryptography is done on a very large scale due to the type of application. While only a few dozen keys can be processed in one design. The key management overhead is medium and can be used by manually processing. However, with a large property, tracking the key expiration time and adjusting the key rotation will quickly become impractical.

Asymmetric Cryptography

Asymmetric cryptography addresses key exchange and scalability issues of symmetric cryptography using a public and private key model. As mentioned, symmetric cryptography is encrypted and decrypted data using a same key, while in asymmetric cryptography; data is encrypted and decrypted using a pair of keys. The public key on the sender side is used to encrypt the data and the private key on the receiver side is used to decrypt it. The idea of this type of cryptography is that the data can be encrypted using its public key, which is freely distributed among all people, and on the other hand, only the person who has access to his private key can decrypt the data.

These two keys are mathematically derived from an original key, which then disappears. Making one key from another without the main key is mathematically impossible. Therefore, everyone can distribute their public key, among other people in the network without compromising their private key. By doing this solution and sharing the public key freely, the problem of key distribution will be solved.

Although it is possible to share public keys in asymmetric cryptography, one of the most important issues in this type of cryptography is the protection of the private key. Therefore, due to the lack of necessary security, no private key should be stored, for example in a web application. In asymmetric cryptography, the processor must be strong and therefore rarely used to encrypt all communications. Instead, asymmetric cryptography is used to swapping session key in most applications, and once the session key is agreed upon, symmetric encryption is used to encrypt the traffic in that session.

Steganography with and without cryptography

As mentioned in section I, the systems are designed to be able to encrypt messages before steganography operations. The question here is, first, what do we need to do the encryption operation before hiding? Second, is the security of steganography algorithms increased by considering cryptographic operations? Third, did not change the entropy of the embedded message using encryption algorithms and the file containing the message will not be suspicious?

In this section, by mentioning two algorithms in image and two algorithms in audio, and its important points, the above questions will be answered. Also, with the evaluations that are done on them, their advantages and disadvantages will be clearly understood.

Steganography must not be confused with cryptography that involves the conversion of the message, so that its meaning is unclear to the malicious people who track it. In this context, the definition of failure of a steganographic system is different from that of a cryptographic system. In cryptography, when an attacker accesses the encryption key and can read the confidential message, the cryptographic system crashes and the algorithm fails. Steganography algorithm failure occurs when an attacker only detects that the stenographic system has been used and that she is able to read the embedded message. According to [1], steganography provides a tool for covert communication between the sender and receiver, which cannot be ignored without a significant change in the data embedded in it. In addition, in classical steganographic systems integrated with cryptographic algorithms, the security of their system depends on the confidentiality of its encrypted algorithm. Therefore, when the encryption system is revealed, the steganography system will fail [4].

Therefore, it can be said that in order to increase the security of the multi-layer, the use of cryptographic algorithms in steganographic systems is always a good idea. However, this will lead to challenges that will be addressed continuation. By combining them, the data can be encrypted by an encryption algorithm and then the ciphertext can be embedded in the image, audio, any other medium with, or none the help of the stage key. As mentioned, the combination of two methods of cryptography and steganography will increase the security of embedded data. But this type of combination will meet needs such as the capacity of the medium, the security of

the embedded data, and the robustness of the combined algorithm for transmission of the secure data over an open channel [7].

Since the purpose of this paper is not to explain steganography and steganalysis algorithms in details, a general explanation is provided for them. In the following, by presenting two steganography algorithms for image and two steganography algorithms for audio, the cryptographic combination with each of these two algorithms is investigated.

The First, algorithm A is explained, so that this algorithm is designed and implemented for both image and audio media. This algorithm is implemented for image and audio on JPEG and WAV format, respectively. This algorithm is implemented using a symmetric encryption operation and without using it with the maximum capacity of the message that can be inserted. In the following, the algorithm B will be explained, so that this algorithm is also designed and implemented on the image media on JPEG format. Also, in section C, an audio algorithm on WAV format is designed and implemented. Similar to the algorithm described in section A, each of the algorithms designed in sections B and C, have been implemented using a symmetric encryption algorithm and without using it with the maximum capacity of the message that can be inserted. Therefore, it is observed that all conditions except the steganography algorithm are considered the same.

As mentioned, one of the most important evaluation criteria in steganography algorithms is to examine ROC curves and confusion matrices, which here, in addition to reviewing them, will be examined the maximum message capacity of both algorithms with and without the use of cryptographic algorithms, and the results will be obtained. Both steganography algorithms are evaluated using steganalysis algorithms and their graphs are examined as follow.

Steganalysis algorithms in image, which are the reference for the two steganography algorithms A and B, examine the features of NJ inter block, NJ intra block, spam, DCTR and CCPEV, for raw and stego media. In [8], a new method of JPEG steganalysis based on observation of the bivariate generalized Gaussian distribution in the Discrete Cosine Transform (DCT) domain is proposed, which extracts the features of the neighboring density inter-block and intra-blocks. In [8], a method for detecting steganography methods is presented in which the insertion operations are performed in the spatial domain by adding a low-amplitude domain independent of the stego signal. In introduced a set of new features for steganalysis of JPEG images. These features are engineered as first-order statistics of quantized noise residues from a decompressed JPEG images using 64 kernels Discrete Cosine Transform (so-called underestimated DCTs). In for the steganalysis JPEG images, the features that are extracted directly from the embedded domain from the DCT coefficients have the best performance. The purpose of this paper is to build a new multi-class JPEG steganalyzer with completely improved performance. They first expand 23 sets of DCT features and then do so by applying calibration to Markov features and reducing their dimensions. The resulting feature set is merged and a 274-dimensional feature vector appears [8-12].

Also, steganalysis algorithms in audio, which are the reference for the two steganography algorithms A and C, examine the various features. In [13], were examined four distance criteria to audio steganalysis, namely perceptual audio quality measure (PAQM), spectral phase distortion (SPD), and log-likelihood ratio (LLR and log-area ratio (LAR). In considered features such as Markov transition and neighboring joint density of the MDCT coefficients. In this paper, IM and INJ marked inter-frame Markov and inter-frame neighboring joint density features [14, 15]. In addition to the mentioned feature set, second-order derivative-based audio steganalysis is done. In, the inter-frame pattern is has changed across adjacent frames. Based on this analysis, they attempted to design feature sets for evaluating frames using second-order derivative based spectrum analysis. The features mentioned. In this paper are: (1) Statistical model and signal complexity that demonstrate the distribution of the violence amount of pixels: Markov random field models (MRFs); Gaussian mixture models (GMMs); and generalized Gaussian density models (GGD) in transform domains. (2) Moment statistics of GGD shape parameter on inter-frame, which is based on spectral distribution analysis, they hypothesized that the hidden behavior mutates the persistence of the distribution of adjacent frames. (3) Frequency-based sub band moment statistics, where second-order derivatives are widespread used for detecting celibate points, margins and so on. The method of extracting signals is based on second-order derivatives statistics: second-order derivatives from 576 MDCT sub band signals through all frames. Calculate statistics, containing mean value, standard deviation, skewness, and kurtosis of sub band signals. Eventually (4) accumulative neighboring joint density and Markov method, where they planned an inter-frame Markov approach (IM) and inter-frame Neighboring Joint Density (INJ) for MP3. In, presented a method that is based on taking advantages of R-MFCC coefficients, which are based Human auditory system. In this paper mentioned Pitch ratio and Mel Scale and Mel-frequency cepstral coefficients metrics. Also considered the feature set including some of above features as custom features that it evaluates for the same dataset [16].

All of the above-mentioned steganalysis algorithms are implemented by MATLAB® and evaluated using ensemble classifier [17].

Algorithm A (Implemented in Image and Audio)

This algorithm is presented in and implemented on JPEG images and wav audios. In this paper, in order to minimize additive distortion in steganographic algorithms, a complete practical method using general (non-binary) embedding operation is proposed. This paper presents a general method for insertion while the performance of the desired additive distortion is minimized with near theoretical performance. They have a complete way to solve finite payload-limited and distortion-limited sender. The implementation

described in this paper adapts them to the problem using standard signal processing tools convolutional codes with trellis quantizer. All of the results summarized at continuation [18].

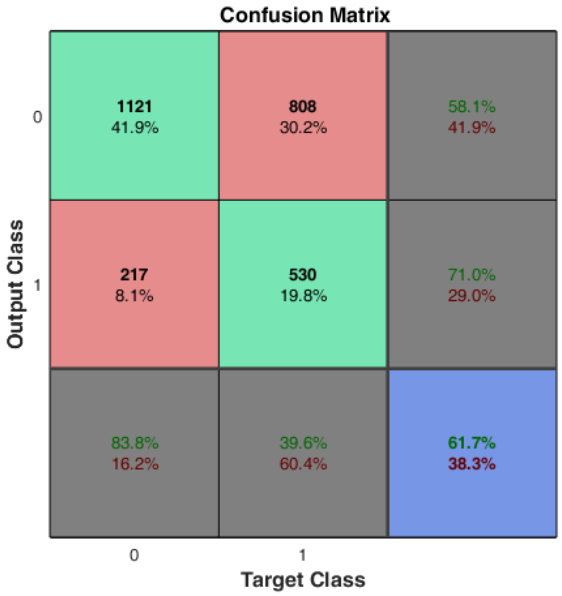

Figure 1: Confusion Matrix Without Using The Cryptographic Algorithm In Image-Algorithm A [18]

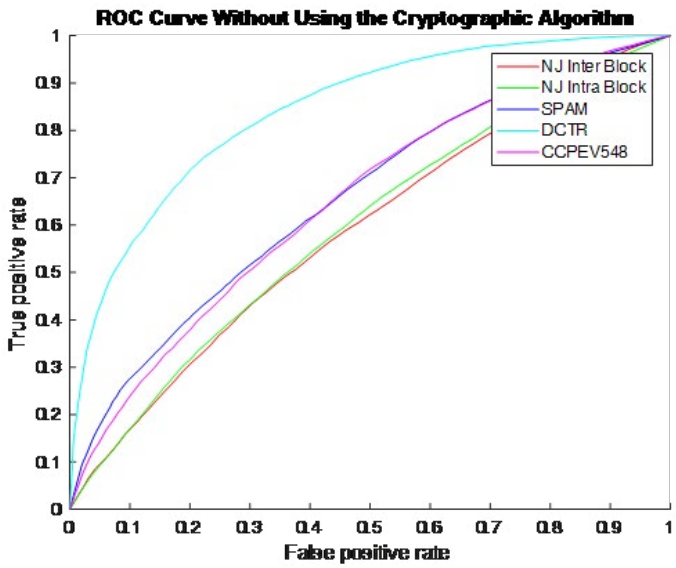

Figure 2: ROC Curve By Maximum Payload Without Using The Encryption Algorithm In Image- Insertion In Algorithm A [18]

Evaluation results without the use of cryptographic algorithm are presented as a confusing matrix of 10, 50 and 100% capacity in all media, which is shown in Fig 1. Also, ROC curves are shown in Fig 2 only with maximum payload without the use of encryption algorithm. In the following in Table 1, the testing error and AUC values are specified for the above-mentioned steganalysis algorithms.

Table 1: Testing Error And AUC Without Using The Encryption Algorithm In Image-Insertion In Algorithm A [18]

Parameters	NJ inter block	NJ intra block	SPAM	DCTR	CCPEV
Testing Error	0.4359	0.4300	0.3925	0.2418	0.3941
AUC	0.5910	0.5975	0.6603	0.8425	0.6530

Table 2 shows maximum payload without using the cryptographic algorithm, which are presented the number of media and their average capacity.

Table 2: Maximum Payload Without Using The Cryptographic Algorithm In Image-Insertion In Algorithm A [18]

The Capacity of Media (Kbit)	2676
Average capacity	5913

Evaluation results with the use of encryption algorithm AES-256 are presented as a confusing matrix of 10, 50 and 100% capacity in all media, which is shown in Fig 3. Also, ROC curves are shown in Fig 4 only with maximum payload with the use of cryptographic algorithm.

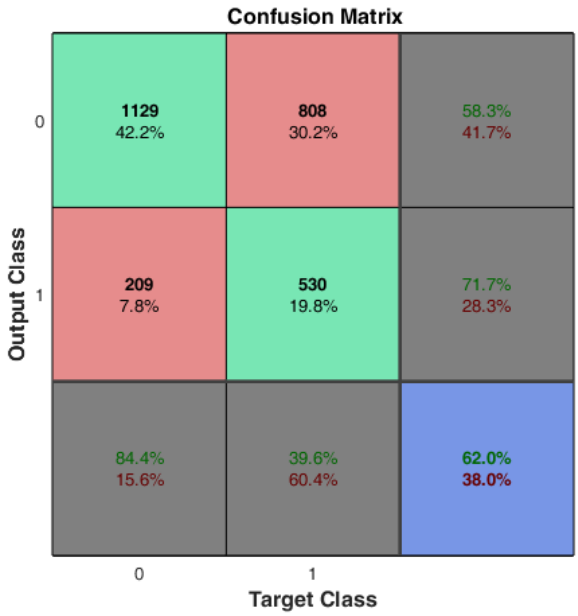

Figure 3: Confusion Matrix With Encryption Algorithm AES-256 in Image-Algorithm A [18]

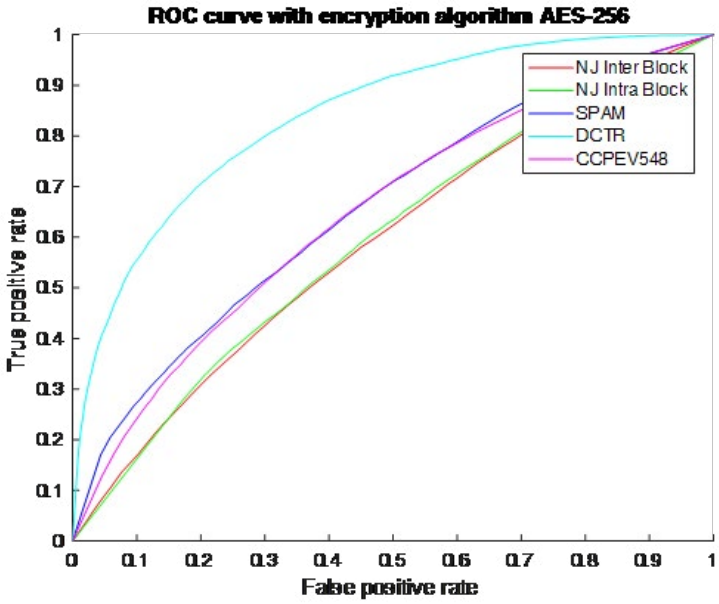

Figure 4: ROC Curve By Maximum Payload With Encryption Algorithm AES-256 In Image-Algorithm A [18]

In the following in Table 3, the testing error and AUC values are specified for the same steganalysis algorithms.

Table 3: Testing Error And AUC With Encryption Algorithm AES-256 In Image-Insertion In Algorithm A [18]

Parameters	NJ inter block	NJ intra block	SPAM	DCTR	CCPEV
Testing Error	0.4355	0.4312	0.3934	0.2459	0.3914
AUC	0.5916	0.5937	0.6595	0.8394	0.6507

Table 4 shows maximum payload with encryption algorithm AES-256, that are presented the number of media and their average capacity.

Table 4: Maximum Payload With Encryption Algorithm AES-256 In Image-Insertion In Algorithm A [18]

The Capacity of Media (Kbit)	2676
Average capacity	5479

Algorithm B (Implemented in image)

This algorithm is designed and implemented quite simply, and so will be no resistance to evaluators. In this paper, the secret message in the LSB method is placed in space Ycbcr of the cover images.

Algorithm 1: JPEG Steganography in domain Y
1: procedure Insertion Operation
Input : $x \in \chi = \gamma^n \cong (0,\cdots,255)^n$
Define : $x_1 = Y\ , x_2 = cb, x_3 = cr$
Return : $x \in \chi = \gamma^n \cong (0,\cdots,255)^n$
2: Convert RGB space to Ycbcr
3: x_1**: flexible by change LSB,** x_2 **: fixed and** x_3 **: fixed**
4: if $x_1 > 128$ **then** $x_1 \leftarrow x_1 + 1$
5: if $x_1 > 128$ **then** $x_1 \leftarrow x_1 - 1$
6: Construct $x = (x_1, x_2, x_3)$
7: Convert Ycbcr to RGB space

Evaluation results in this algorithm without the use of cryptographic algorithm are presented as a confusing matrix of 10, 50 and 100% capacity in all media, which is shown in Fig 5. Also, ROC curves are shown in Fig 6 only with maximum payload without the use of encryption algorithm.

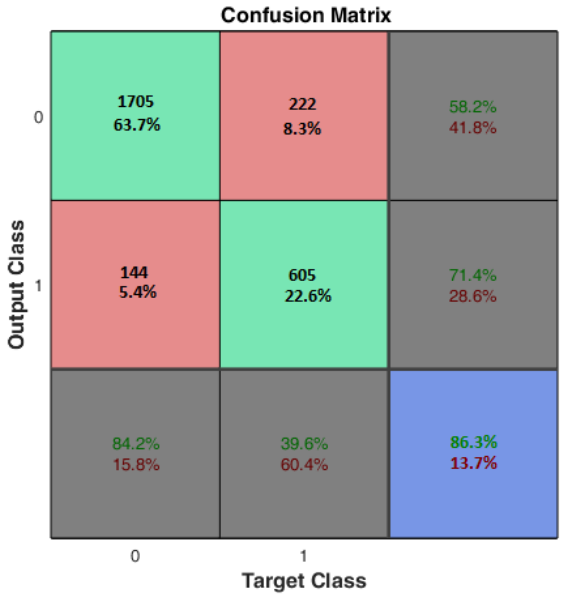

Figure 5: Confusion Matrix without Using the Cryptographic Algorithm in Image-Algorithm B

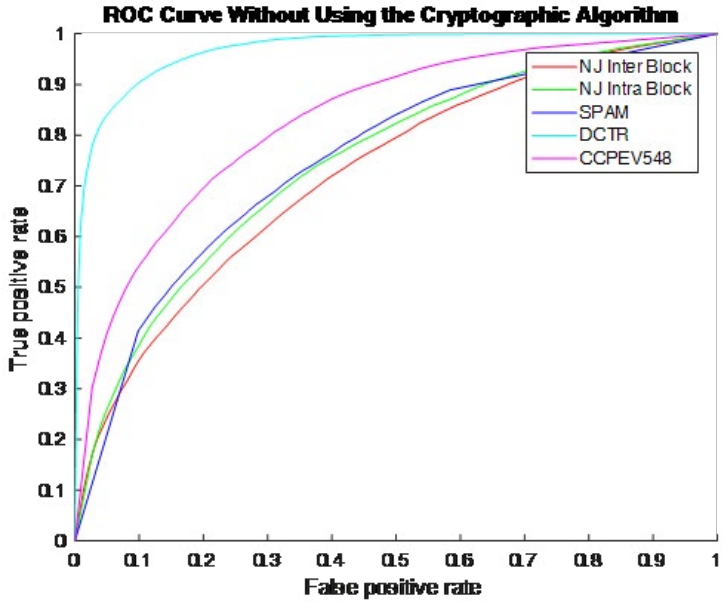

Figure 6: ROC Curve by Maximum Payload without Using the Encryption Algorithm in Image-Insertion in Algorithm B

In the following in Table 5, the testing error and AUC values are specified for the above-mentioned steganalysis algorithms.

Table 5: Testing Error and AUC without Using the Encryption Algorithm in Image-Insertion in Algorithm B

Parameters	NJ inter block	NJ intra block	SPAM	DCTR	CCPEV
Testing Error	0.3388	0.3173	0.3109	0.0980	0.2504
AUC	0.7266	0.7488	0.7536	0.9692	0.8318

Table 6: Maximum Payload without Using the Cryptographic Algorithm in Image-Insertion in Algorithm B

The Capacity of Media (Kbit)	2676
Average capacity	5479

Table 6 shows maximum payload in this algorithm without using the cryptographic algorithm, which are presented the number of media and their average capacity.

Evaluation results in this algorithm with the use of encryption algorithm AES-256 are presented as a confusing matrix of 10, 50 and 100% capacity in all media, which is shown in Fig 7. In addition, ROC curves are shown in Fig 8 only with maximum payload with the use of cryptographic algorithm.

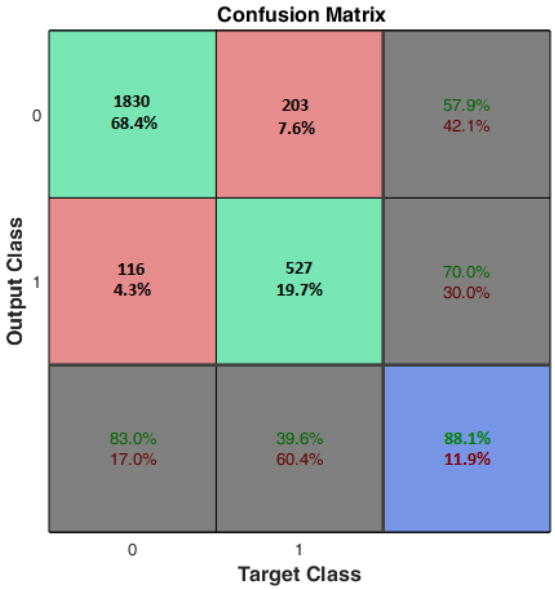

Figure 7: Confusion Matrix with Encryption Algorithm AES-256 in image-Algorithm B

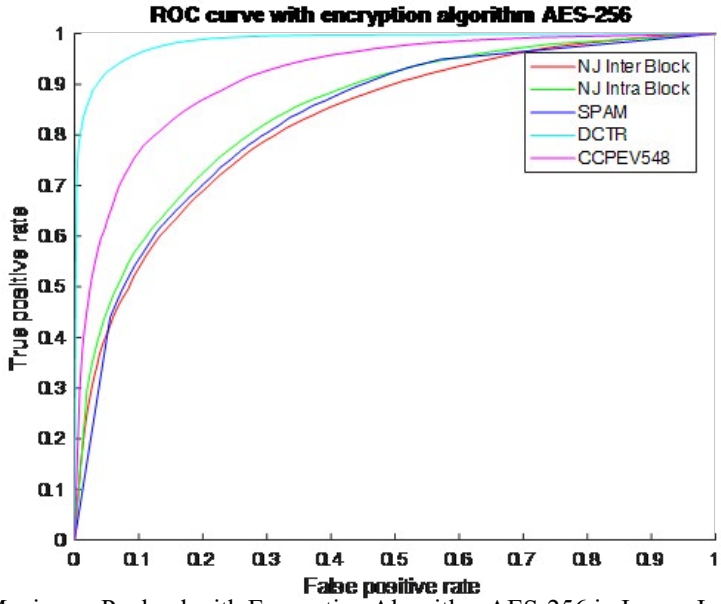

Figure 8: ROC Curve by Maximum Payload with Encryption Algorithm AES-256 in Image-Insertion in Algorithm B

In the following in Table 7, the testing error and AUC values are specified for the same steganalysis algorithms. Table 8 shows maximum payload in this algorithm with encryption algorithm AES-256, that are presented the number of media and their average capacity.

Table 7: Testing Error and AUC with Encryption Algorithm Aes-256 in Image-Insertion in Algorithm B

Parameters	NJ inter block	NJ intra block	SPAM	DCTR	CCPEV
Testing Error	0.2532	0.2347	0.2456	0.0636	0.1618
AUC	0.8266	0.8473	0.8333	0.9854	0.9175

Table 8: Maximum Payload with Encryption Algorithm AES-256 in Image-Insertion in Algorithm B

The Capacity of Media (Kbit)	2676
Average capacity	6347

By viewing the Fig 2, 4 and Table 1, 3 it can be seen that if the steganography algorithm is designed in such a way that the ROC is acceptable to most of the steganalysis algorithms, the use of the cryptographic algorithm can give it a higher security factor. But if the steganography algorithm is designed in such a way that the ROC does not have acceptable over most of the steganalysis algorithms, using a cryptographic algorithm will not only increase its security factor, but will also make it more suspicious than its images (media). This point can be clearly seen by looking at Fig 6, 8 and Table 5, 7.

Also, by viewing the Table 2, 4 in algorithm A and Table 6, 8 in algorithm B it can be seen that the capacity of the message is one of the disadvantages of using cryptographic algorithms in steganography. As can be seen in each of the above algorithms, the use of the AES encryption algorithm has made the capacity of the inserted message less than when this algorithm is not used. Therefore, it can be said that in some cryptographic algorithms that change the size of the main message after encryption operation, their use in steganography algorithms will reduce the capacity of the insertable message.

Algorithm C (Implemented in audio)

This algorithm is presented in and implemented on wav audios. In this paper, a wav audio file is received and placed at the least significant bit of message as binary form [19].

Algorithm 2: WAV Steganography in LSB	
1: procedure Insertion Operation	
	Input : $x \in \chi = \gamma^n \cong (-1,\cdots,1)^n$
	Return : $x \in \chi = \gamma^n \cong (-1,\cdots,1)^n$
2:	$x \leftarrow u \operatorname{int} 8(255.(x + 0.5))$
3:	$LSB(x) \leftarrow binary(message)$
4:	$x \leftarrow (double(x)/255) - 0.5$

The work process is as follow. Samples of each data are extracted by obtaining a sample rate of that audio and it is considered as input data by adding 0.5 units. It then inserts each of the message bits from the beginning of the audio into the least significant bit of the audio, and finally written the data and creates the stego file by adding the same 0.5 unit to data sample. As can be seen, this algorithm is designed and implemented quite simply, and so will be no resistance to evaluators and it has many weaknesses.

The dataset used in the implementation of this paper is the TIMIT dataset, which is considered to be the most difficult condition for steganography because it is produced in particularly acoustic methods [20]. The TIMIT data set of etude speech has been created by the voices of several individuals' men and women to provide speech data for acoustic-phonetic investigation studies and for the assessment of automatic speech distinction systems. This data set is recorded with very high quality so that there are 630 people or speakers who speak with 8 different dialects of American English in which each person has read 10 phonetically rich sentences.

By referring to algorithm A, and this time implementing it in wav format, the following results will be obtained.

Like before, evaluation results without the use of cryptographic algorithm are presented as a confusing matrix of 10, 50 and 100% capacity in all audio media, which is shown in Fig 9. In addition, ROC curves are shown in Fig 10 only with maximum payload without the use of encryption algorithm.

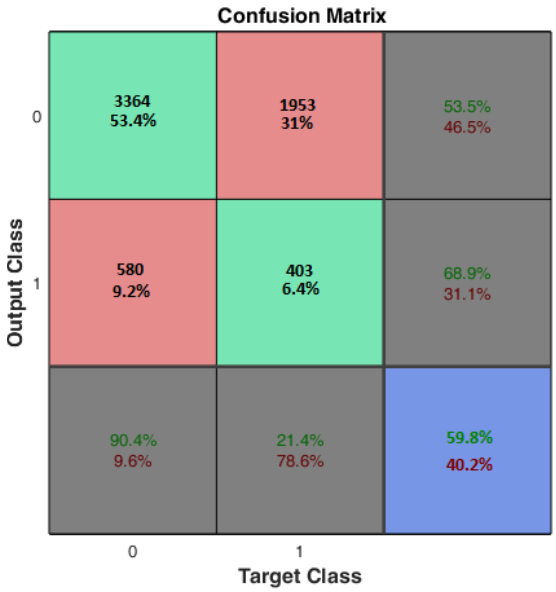

Figure 9: Confusion Matrix Without Using The Cryptographic Algorithm In Audio-Algorithm A [18]

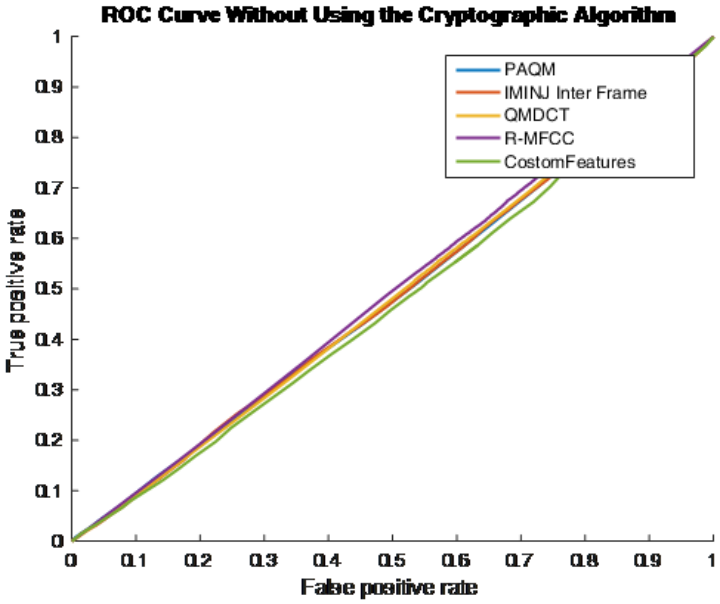

Figure 10: ROC Curve By Maximum Payload Without Using The Encryption Algorithm In Audio-Algorithm A [18]

In the following in Table 9, the testing error and AUC values are specified for the above-mentioned steganalysis algorithms in audio media. In addition, Table 10 shows maximum payload without using the cryptographic algorithm, which are shown the number of media and their average capacity for TIMIT dataset.

Table 9. Testing Error and AUC without Using the Encryption Algorithm in Audio-Insertion in Algorithm a [17]

Parameters	Footprints	IMINJ	QMDCT	RMFCC	Custom Features
Testing Error	0.4892	0.4871	0.4813	0.4799	0.4991
AUC	0.5108	0.5129	0.5187	0.5201	0.5009

Table 10: Maximum Payload Without Using The Cryptographic Algorithm In Audio-Insertion In Algorithm A [18]

The Capacity of Media (Kbit)	6300
Average capacity	93456

In follow, evaluation results with the use of encryption algorithm AES-256 are presented as a confusing matrix of 10, 50 and 100% capacity in all audio media, which is shown in Fig 11. In addition, ROC curves are presented in Fig 12 only with maximum payload with the use of cryptographic algorithm.

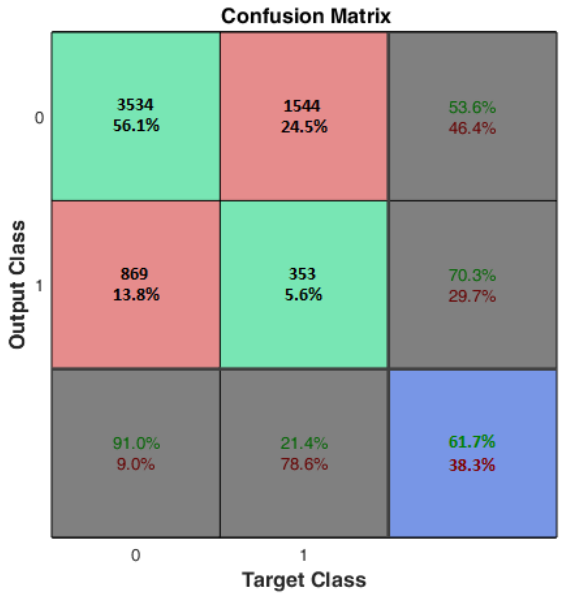

Figure 11: Confusion Matrix With Encryption Algorithm AES-256 In Audio-Algorithm A [18]

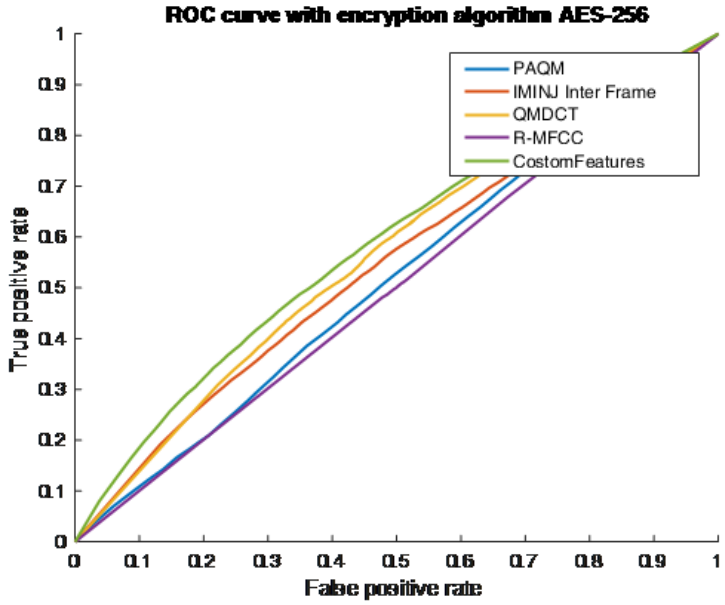

Figure 12: ROC Curve By Maximum Payload With Encryption Algorithm AES-256 In Audio-Algorithm A [18]

Therefore, in Table 11, the testing error and AUC values are specified for the same steganalysis algorithms in audio media. Table 12 presented maximum payload with encryption algorithm AES-256, that are shown the number of media and their average capacity for the same TIMIT dataset.

Table 11: Testing Error And AUC With Encryption Algorithm Aes-256 In Audio-Insertion In Algorithm A [18]

Parameters	Footprints	IMINJ	QMDCT	RMFCC	Custom Features
Testing Error	0.4453	0.4284	0.4175	0.4617	0.4046
AUC	0.5547	0.5716	0.5825	0.5383	0.5954

Table 12: Maximum Payload With Encryption Algorithm AES-256 In Audio-Insertion In Algorithm A [18]

The Capacity of Media (Kbit)	6300
Average capacity	88209

Now, we will evaluate algorithm C. Evaluation results in algorithm C without the use of cryptographic algorithm are presented as a confusing matrix of 10, 50 and 100% capacity in all audio media, which is presented in Fig 13. Also, ROC curves are shown in Fig 14 only with maximum payload without the use of encryption algorithm.

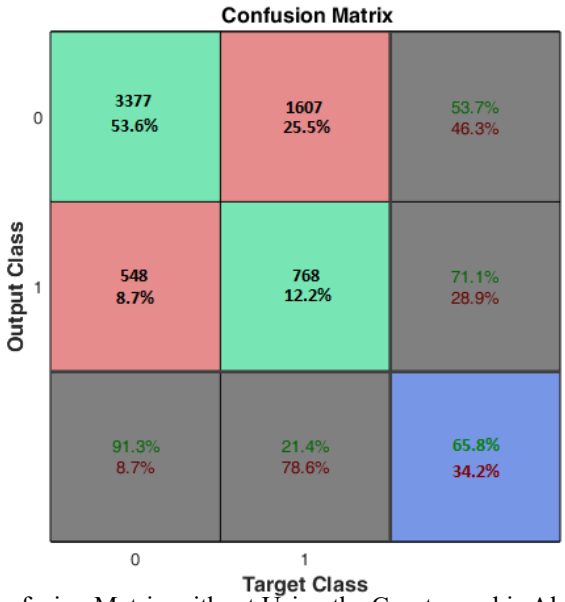

Figure 13: Confusion Matrix without Using the Cryptographic Algorithm in Audio-Algorithm C

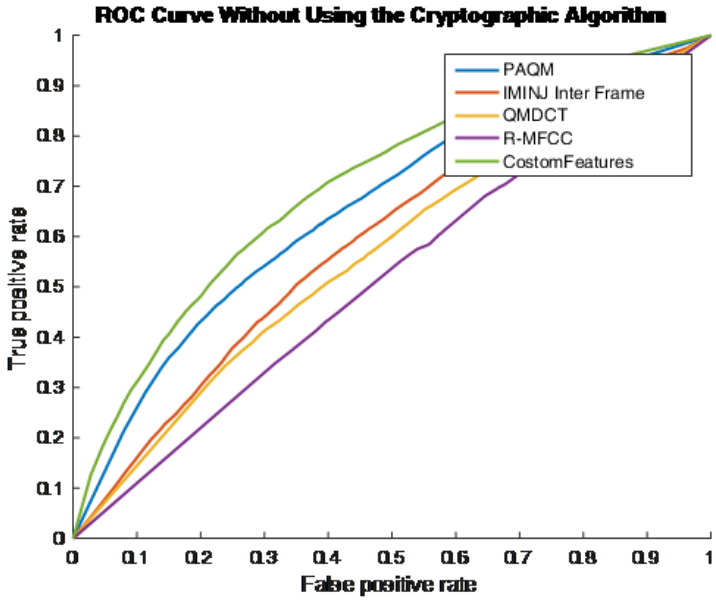

Figure 14: ROC Curve by Maximum Payload without Using the Encryption Algorithm in Audio-Algorithm C

In the following in Table 13, the testing error and AUC values are specified for the above-mentioned steganalysis algorithms for audio media. Table 14 shows maximum payload in this algorithm without using the cryptographic algorithm, which are shown the number of media and their average capacity.

Table 13: Testing Error and AUC without Using the Cryptographic Algorithm in Audio-Insertion in Algorithm C

Parameters	Footprints	IMINJ	QMDCT	RMFCC	Custom Features
Testing Error	0.3983	0.4336	0.4421	0.4793	0.3689
AUC	0.6017	0.5664	0.5579	0.5207	0.6311

Table 14: Maximum Payload without Using the Cryptographic Algorithm in Audio-Insertion in Algorithm C

The Capacity of Media (Kbit)	6300
Average capacity	12568

Evaluation results in this algorithm with the use of encryption algorithm AES-256 are presented as a confusing matrix of 10, 50 and 100% capacity in all audio media, which is shown in Fig 15. Also, ROC curves are shown in Fig 16 only with maximum payload with the use of cryptographic algorithm.

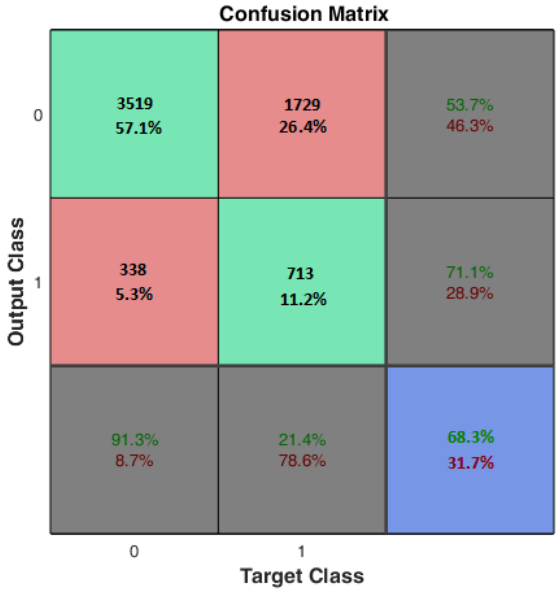

Figure 15: Confusion Matrix with Encryption Algorithm AES-256 in Audio-Algorithm C

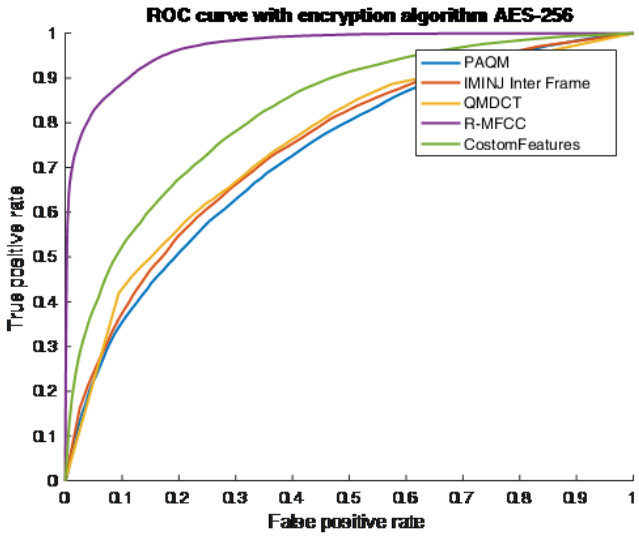

Figure 16: ROC Curve by Maximum Payload with Encryption Algorithm AES-256 in Audio-Algorithm C

Then in Table 15, the testing error and AUC values are specified for the same steganalysis algorithms for audio media. Table 16 is presented maximum payload in this algorithm with encryption algorithm AES-256, that are shown the number of media and their average capacity.

Table 15: Testing Error and AUC with Encryption Algorithm AES-256 in Audio-Insertion in Algorithm C

Parameters	Footprints	IMINJ	QMDCT	RMFCC	Custom Features
Testing Error	0.2533	0.2405	0.2393	0.0893	0.1644
AUC	0.7467	0.7595	0.7607	0.9107	0.8356

Table 16: Maximum Payload with Encryption Algorithm AES-256 in Audio-Insertion in Algorithm C

The Capacity of Media (Kbit)	6300
Average capacity	11876

By viewing the Fig 10, 12 and Table 9, 11 it can be seen that if the steganography algorithm is designed in such a way that the ROC is acceptable to most of the steganalysis algorithms, the use of the cryptographic algorithm can give it a higher security factor. But if the steganography algorithm is designed in such a way that the ROC does not have acceptable over most of the steganalysis algorithms, using a cryptographic algorithm will not only increase its security factor, but will also make it more suspicious than its images (media). This point can be clearly seen by looking at Fig 14, 16 and Table 13, 15.

Also, by viewing the Table 10, 12 in algorithm A and Table 14, 16 in algorithm C it can be seen that the capacity of the message is one of the disadvantages of using cryptographic algorithms in steganography. As can be seen in each of the above algorithms, the use of the AES encryption algorithm has made the capacity of the inserted message less than when this algorithm is not used. Therefore, it can be said that in some cryptographic algorithms that change the size of the main message after encryption operation, their use in steganography algorithms will reduce the capacity of the insertable message.

Conclusion

After describing the definitions of cryptography and steganography, how to use them in specific applications and the combination of these two technologies were discussed. The use of cryptographic algorithms in steganographic algorithms will have advantages and disadvantages that can be examined and observed in ROC curves and confusion matrices by steganalysis algorithms. Also, the maximum capacity that can be included in the use and non-use of cryptographic algorithms in steganographic algorithms is another challenge that should be examined considering security vs capacity. In this paper, it was shown that if the cryptographic algorithm changes the size of the original message after encryption operation, its use in steganography algorithms both in image and in audio media will reduce the capacity of the insertable message.

Acknowledgments

We are enclosing a manuscript entitled: "Analysis of Cryptography before Steganography Operation by ROC Curves and Confusion Matrices Criteria" by Ali Hadipour, Raheleh Afifi and Hamed ShojaeiYas, to be considered for publication in your journal, Journal of Electrical Electronics Engineering.

The manuscript is the result of research activity and implementation of a practical example in using of a cryptography algorithm in the steganography system that is sent for evaluation. It should be noted that the authors of the paper have a history of publishing various papers in the field of data security.

This research was supported by Isfahan Mathematics House. We thank our colleagues from Cryptography and coding Department who provided insight and expertise that greatly assisted the research, although they may not agree with all of the conclusions of this paper.

All authors have participated in the study and concur with the submission and subsequent revisions submitted by the corresponding author.

Author Contributions Statement

Ali Hadipour researched and wrote the main manuscript text and Raheleh Afifi all figures and Hamed Shojaeiyas prepared all tables. All authors reviewed the manuscript.

Funding Statement

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Conflict of Interest Statement

All authors declare that they have no conflicts of interest.

Data Availability Statements

The datasets generated analyzed during the current study are not publicly available due to secrecy, but are available from the corresponding author on reasonable request.

References

1. V. Jain,. (2012). "Public-key steganography based on modified LSB method," Journal of Global Research in Computer Science, vol. 3, no. 4, pp. 26-29.
2. Abikoye Oluwakemi, C., Adewole Kayode, S., & Oladipupo

Ayotunde, J. (2015). Efficient data hiding system using cryptography and steganography. International Journal of Applied Information Systems IJAIS411 pp. 6, 11.
3. Jayaram, P., Ranganatha, H. R., & Anupama, H. S. (2011). Information hiding using audio steganography–a survey. The International Journal of Multimedia & Its Applications (IJMA) Vol, 3, 86-96.
4. Joseph, A., & Sundaram, V. (2017). Cryptography and steganography–A survey.
5. Ren, Y., Cai, S., & Wang, L. (2021). Secure AAC steganography scheme based on multi-view statistical distortion (SofM-vD). Journal of Information Security and Applications, 59, 102863.
6. Hadipour, A., Sajadieh, S. M., & Afifi, R. (2020). Jump Index in T-functions for designing a new basic structure of stream ciphers. Cryptology ePrint Archive.
7. Provos, N., & Honeyman, P. (2003). Hide and seek: An introduction to steganography. IEEE security & privacy, 1(3), 32-44.
8. Liu, Q., Sung, A. H., & Qiao, M. (2009, October). Improved detection and evaluation for JPEG steganalysis. In Proceedings of the 17th ACM international conference on Multimedia (pp. 873-876).
9. Pevny, T., Bas, P., & Fridrich, J. (2010). Steganalysis by subtractive pixel adjacency matrix. IEEE Transactions on information Forensics and Security, 5(2), 215-224.
10. Holub, V., & Fridrich, J. (2014). Low-complexity features for JPEG steganalysis using undecimated DCT. IEEE Transactions on Information forensics and security, 10(2), 219-228.
11. Pevny, T., & Fridrich, J. (2017, March). Merging Markov and DCT features for multi-class JPEG steganalysis. In Security, steganography, and watermarking of multimedia contents IX (Vol. 6505, pp. 28-40). SPIE.
12. Kodovský, J., & Fridrich, J. (2008, March). Influence of embedding strategies on security of steganographic methods in the JPEG domain. In Security, Forensics, Steganography, and Watermarking of Multimedia Contents X (Vol. 6819, pp. 13-25). SPIE.
13. Özer, H., Sankur, B., Memon, N., & Avcıbaş, İ. (2006). Detection of audio covert channels using statistical footprints of hidden messages. Digital Signal Processing, 16(4), 389-401.
14. Kuriakose, R., & Premalatha, P. (2015). A novel method for MP3 steganalysis. In Intelligent Computing, Communication and Devices (pp. 605-611). Springer, New Delhi.
15. Wang, Y., Yang, K., Yi, X., Zhao, X., & Xu, Z. (2018, June). CNN-based steganalysis of MP3 steganography in the entropy code domain. In Proceedings of the 6th ACM Workshop on Information Hiding and Multimedia Security (pp. 55-65).
16. Ghasemzadeh, H., & Khalil Arjmandi, M. (2017). Universal audio steganalysis based on calibration and reversed frequency resolution of human auditory system. IET Signal Processing, 11(8), 916-922.
17. Harine Rajashree, R., & Hariharan, M. (2021). A Study on Ensemble Methods for Classification. In Machine Learning, Deep Learning and Computational Intelligence for Wireless Communication (pp. 127-136). Springer, Singapore.
18. Filler, T., Judas, J., & Fridrich, J. (2011). Minimizing additive distortion in steganography using syndrome-trellis codes. IEEE Transactions on Information Forensics and Security, 6(3), 920-935.
19. Abdulkadhim, H. A., Shehab, J. N., & Albu-rghaif, A. N. (2018, December). audio security based on LSB steganography and 4-D Lü system. In 2018 Third Scientific Conference of Electrical Engineering (SCEE) (pp. 203-208). IEEE.
20. Garofolo, J. S. (1993). Timit acoustic phonetic continuous speech corpus. Linguistic Data Consortium, 1993.