Combining Encryption and Preservation in Information Security to Secure Sending a Message

Sameer Nooh
snooh@ut.edu.sa
Department of Computer Science, Tabuk University, Umluj, Saudi Arabia

Abstract
With the growing exchange of data between individuals and institutions through various electronic communication, valuable data protection is in high demand to ensure that it is not hacked and that privacy is protected. Many security techniques, such as encryption and steganography, have emerged to prevent security breaches. The purpose of this research is to integrate cryptographic and steganography techniques to secure text message sending. The Rijndael algorithm was used to encrypt the text message, and the Least Significant Bit algorithm was also used to hide the encrypted message in a color image. Experiments on the suggested method have proven that it can improve the security of sent messages due to the human eye's inability to identify the original image from the image after it has been covered, as well as the encryption of the message using a password.

Keywords:
Information Security – Encryption –Inform-ation Technology – Steganography - Sending Message.

1. Introduction:

With the continuous development in the field of computers and communications, the need for users of various classifications to exchange data and send it through various media from one place to another around the world, and after the emergence of the Internet, and as a result of the great development that occurred in its applications, it became the most common medium for exchanging data, as There are a variety of ways to send data over the internet, including email., chats, social media...etc. As the Internet is a public network that everyone can access and view data in, sending data through it faces several problems, including the problem of the security threat, Personal or confidential information can be stolen or hacked in a variety of ways. Because a good communication system provides three important characteristics: confidentiality, reliability, and safety (kobayashi, et al., 2009).

Confidentiality ensures that only authorized individuals have the right to access the information exchanged. Reliability allows verification of the origin and owner of the information exchanged, while integrity ensures that the information exchanged is not modified or tampered with.

Confidentiality is necessary to prevent illegal access to transmitted data, since reliability Integrity is required to verify ownership and detect tampering with received data. Because the previous three characteristics are achieved by protecting and securing information circulated through the eyes of various communications, information security has received great attention in the past few decades, as many Internet crimes such as forgery, modification, and piracy have reached dangerous levels, and therefore the issue of information security has remained Worrying and needs renewable solutions. From here, the need to protect confidential and important information increased, which led to the emergence of cryptography to achieve this, and it is considered one of the well-known and popular solutions for data protection. Using the concept of encryption, the message becomes unreadable, as the encryption of digital media such as audio, image, and video achieves a high protection rate, but the encryption of digital messages makes it attractive to intruders as it is sent in a clear encrypted form without hiding it, which indicates its importance. Despite the development that accompanied cryptography and its techniques, using various encryption algorithms that are constantly developing, in return, algorithms and methods are constantly being developed to decrypt and steal data sent over the Internet, which led to the loss of privacy and confidentiality of data, and this called for the search for other methods to protect Digital messages, such as steganography, which is a good way to bypass the problem of data clarity during transmission (Fouad, 2017 p. 545).

Information Steganography appeared to provide a new tool that contributes to increasing the security and confidentiality of information and relies on hiding (embedding) information within the information carrier so that the message is known only to the authorized (sender and recipient). , and is not known by hackers or intruders and they cannot be aware of it.

In general, the purpose of encryption is to protect the confidentiality and integrity of the transmitted message by encrypting its contents, while data steganography seeks to achieve the same goal by hiding the bits of the transmitted message within the bits of the host medium (Zinaly, et al., 2017). This research seeks to combine between encryption and masking techniques to increase the security of a text message while sending it through various means of communication.

Manuscript received April 5, 2022
Manuscript revised April 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.4.35

2.The problem of Research:

The research problem is represented in the ability of intruders on communication networks and intruders to penetrate these networks despite the presence of means of protection against intrusions such as passwords and firewalls, and their ability to decipher encrypted messages that are exchanged through these networks despite the development and constant updating of encryption algorithms, which led To the growing need for alternatives and other tools that make it more difficult for these hackers to access data and know its content, and this need increases as the importance and confidentiality of this data increases.

3.The objective of Research:

The aim of the research is to review the different data encryption and masking algorithms and apply one of the hiding algorithms to text messages after encrypting them using one of the encryption algorithms; to hide it inside a color image. The two algorithms applied in this research are the Rijndael algorithm for encryption and the Least Significant Bit (LSB) algorithm for masking. These two algorithms will be applied using VB.Net on a different set of images and texts of different lengths, to determine the ability of this mechanism to increase the protection of data from intruders when it is sent between users, and to retrieve it later in a way that preserves the original text as it is unchanged.

3.1Firstly: Information Security:

Information security includes three components (Kandilji, et al., 2012, pp. 175-176):

a. Confidentiality of Information: This aspect includes all necessary measures to prevent unauthorized persons from accessing sensitive or confidential information.

B. Integrity and security of information: i.e. taking the necessary measures to protect information from alteration.

c. Ensuring access to information and computer resources: that is, information is always available to those authorized to access it.

The system can be considered safe or unsafe if it achieves the main characteristics of the information when circulating this information, which in its entirety is related to protecting the information from penetration with the aim of stealing or tampering, and these characteristics include availability, accuracy, reliability or health Authenticity, Confidentiality, Integrity. (Whitman, et. Al., 2012).

3.2 Secondly: Security Attacks:

The data is sent from the source to the target (destination), which is referred to as normal data flow. But it is possible for some attackers (hackers) to penetrate the network for the purpose of accessing or modifying the original data, and this is known as security attacks, where the attacker can interrupt this natural flow of data by implementing various hacking techniques on the data and the carrier network, such as interruption, and interception (Interception, modification, and fabrication). All these types of attacks, if they occur, make the system insecure, and therefore unable to achieve the main characteristics of the information.

With these security breaches trying to change the original data, protecting data from breach becomes an ongoing task for any organization or individual sending data, by implementing several security measures or methods including prevention, detection, response and recovery.

3.3. Thirdly: Ways of Security Attacks Prevention:

There are different systematic approaches to preventing security attacks, which are as follows:

3.4 Cryptography:

"The word cryptography is derived from the Greek language and consists of two syllables: Crypto, which means secret, and graphy, which means writing, meaning secret writing" (Hussein, 2010, pg. 43). Encryption is defined as: "the process of encoding a message so that its meaning is incomprehensible" (Al-Hamami, et al., 2007). Thus, it is the process of mixing or distorting the original text by rearranging and replacing the original text and organizing it to appear unreadable by others. It is an effective way to protect the information sent through the network.

The science of cryptography and cipher analysis is known as cryptology. Cryptography is a means of conveying messages to a target in a secret and secure manner. Cryptology is a method of obtaining the original texts from the messages in which those texts are contained (Whitman, et al., 2012)

In general, encryption is the sending of data from the source to the target after it has been modified using a security code. Encryption systems use the original text and a secret key as input and use a specific encryption algorithm to generate a ciphertext.

3.5 The most important elements of coding are:

a. Plain text: The original piece of information to be sent to the target.

B. Encryption algorithm: It is the basic key of any encryption system. The encryption algorithm allows for many substitutions and modifications to the original text.

c. Secret key: means by user, and is an input to the encryption algorithm, which performs many replacements and modifications differently based on that key.

D. Cipher Text: represents the output of the encryption algorithm. It is a mixed text, and varies each time depending on the secret key given to the encryption algorithm.
Encryption work is related to finding algorithms used to achieve the following:

- Hide the content of messages from everyone except those authorized to provide privacy and confidentiality.
- Validate messages that the recipient has any authorization.

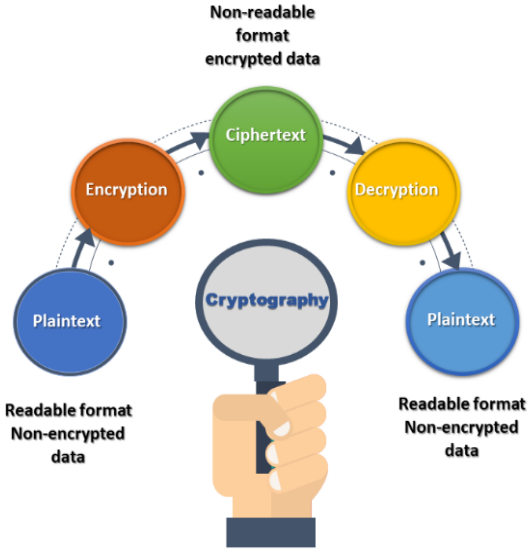

Figure No (1): it demonstrates the elements of cryptography

3.6 Fourthly: Cryptographic Algorithms:

There are several encryption algorithms that differ according to the type of encryption used, and they can be divided according to the encryption standard used into two types (Stallings, 2013):

a. Algorithm for symmetric encryption:

This is known as public-key encryption. In it, the encryption and decryption processes are carried out with two different keys, one for encryption and another key for decryption.

In asymmetric encryption, data encrypted with a public key can only be decrypted with the same algorithm, and a message encrypted with a private key can only be decrypted with the corresponding public key.

The main problem with asymmetric encryption is the cipher key. Whenever two different people want to exchange data at the same time using asymmetric encryption, they both need four different keys (two each). It gets even more confusing, as each file needs the corresponding key to be opened.

b- Algorithm for symmetric encryption:

It is encryption that is carried out using a single key and is known as Conventional Encryption, also known as Private key Cryptography. In general, the symmetric encryption algorithm uses the same key for encryption and decryption. The level of security of this type of encryption also depends on the length of the key, it is It increases with the length of the key.

3.7 Fifthly: Types of analogue encryption algorithms:

- **Data Encryption Standard (DES):**

This algorithm uses a 56-bit key, and therefore cannot be parsed by the hacker. Therefore, the problem of cipher pickling is avoided when using this algorithm. But what hinders this algorithm is a brute-force attack.

- **Rijndael - AES (Rijndael-Advanced encryption Standard):**

The Rijndel algorithm re-encrypts a block according to the block size and key length. In it, for example, 128-bit blocks are used as inputs and result in encrypted blocks of the same size, i.e. 128 bits. It supports blocks and keys of different sizes such as 128, 192, and 256-bit keys. The size of the encryption key determines the number of bits and complexity of the ciphertext, and the ciphertext generated in the middle of the return process is called State, which is a square array of four rows and the number of columns equals the length of the block divided by 32. As shown in Table (1), as shown in Figure 1 is the structure of the Rijndel algorithm.

Table (1) AES cycles by key length (kevin, 2015)

User AES	Key Length	Block Size	Number of Courses
AES – 128	4	4	10
AES – 192	6	4	12
AES - 256	8	4	14

There are four main steps that take place in each cycle of the Rijndel algorithm, as shown in Figure (2), which are:
A. Sub byte substitution.
B. Line offset (Shift Row).

c. Mix Column.
D. Add Round Key.
Rijndel's algorithm is widely accepted due to its strong encryption, complex processing, and resistance to brute force attacks.

3.8 Sixthly: Block Cipher Modes:

It specifies the type of cipher block to be used to encrypt data.

There are a number of types of cipher blocks, the most important and most widely used is CBC Cipher Block Chaining, and they work as follows:
a. Before encoding the first block of the original text is encoded with an initial randomization vector IV (Initialization Vector) by XORing it.
B. Before encrypting each block of the original text it is enclosed with the ciphertext of the previous block by XORing it.
c. If the original text has multiple known or duplicate blocks, each block will be encoded into a different ciphertext block.

1. Decryption algorithm:

It is the reverse of the encryption process. It takes both the cipher text and the secret key as input and results in the original text as output.

2. Steganography:

Steganography comes from the Greek word which means "covered writing." It's the process of hiding a piece of data within another source of data, such as a text, image, audio, or video file, so that it's both visible and invisible. There are a number of carrier-based data masking techniques.

Steganography is a Greek word consisting of two syllables (stegano meaning covered, and graph meaning writing or drawing, and these two syllables together mean the term security writing or covered writing). (Abdullah, 2009).

Stealth can be defined as “the process of concealing confidential or sensitive information within another carrier in such a way that no one except authorized users can discover the presence of a secret message within it” (Whitman, et. Al., 2012). Thus, it is the process of hiding a piece of information, inside another information source, such as: text, image, audio or video file, to be invisible and not visible. There are several carrier-based data masking techniques.

Hiding supports another type of digital format that is used to hide data such as image, audio, and video files, acting as vectors to send private and important messages to the recipient to eliminate security vulnerabilities. Masking techniques can be implemented using different file formats such as: audio files (.mp3, WMV..etc), video (.mpeg., .dat..etc), and images (.jpeg., bmp..,...etc).

However, images are still the most widely used files in cloaking techniques. At present, there are a number of algorithms that help in implementing masking applications on them.

Encryption and cloaking are used together for the purpose of sending data securely. The method used in hiding is the same as in encryption in terms of the stages, encryption, decryption and the secret key. The difference is that in cloaking the message is kept securely without any changes in it, but in cryptography the original content of the message varies with different stages such as encryption and decryption.

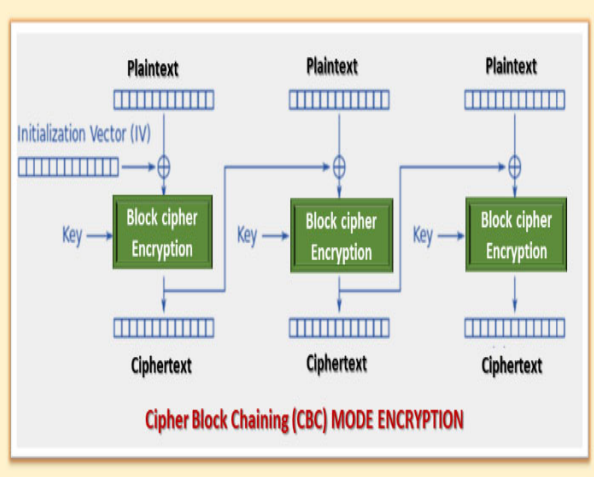

Figure No (2): it illustrates the cipher block chaining mode encryption

3.9 Seventhly: Types of Steganography:

There are different types of steganography techniques which are (Abdullah, 2009):

A. Pure Steganography:

It is the process of including data in the object without any private keys, and this type of steganography depends heavily on confidentiality.

This type of steganography does not provide sufficient security because the message is easy to retrieve if the unauthorized person knows the embed method. But one of its advantages is that it reduces the difficulty of sharing the key.

B. Secret Key Steganography:

It is another type of steganography that uses the same procedure except for the use of secret keys. This type uses a single (independent) key to hide data inside the object which is similar to a symmetric key. The rollback uses the same key as the hide.

This type of steganography is more secure compared to mere concealment, and its main problem lies in sharing the

secret key. If the hacker knows the key, it will be easy for him to retrieve and access the original information.

C. **Steganography using a Public Key:**

It uses two types of keys. One is a steganographic private key, while the other is a retrieval public key that is stored in a public database.

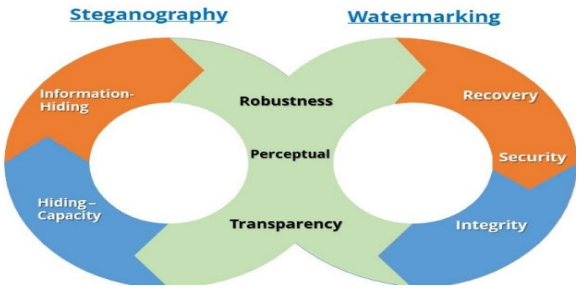

Figure No (3): it clarifies the basics of Steganography

3.10 Eighthly: Steganography Algorithms:

Table (2) presents a comparison of those algorithms:
Table (2) Comparison of Algorithms

Steganography	Speed	Quality of Steganography	Security
LSB	High	Good	Less
F5	High	The highest and up to 13.4%	High and strong
JSteg	High	Embedding capacity up to 12%	less

There are many algorithms used to hide data, including (Andrews, et. al., 2013):

A. JSteg Algorithm.
B. F5 algorithm.
C. LSB (Least Significant Bit Algorithm)
D. Steganography& Seek: The Randomised Approach.
E. OutGuess Algorithm 0.1.F. F3 algorithm.

A. J . (JSteg Algorithm):

The JSteg algorithm is used to embed messages in lossy compressed JPEG images, as it has a high embedding capacity of 12%. It is an algorithm that is resistant to visual attacks but less immune to statistical attacks. This algorithm only guarantees within JPEG images since the content of these images is centered in the image frequency coefficients to achieve storage in a very compressed form.

B. F5 Algorithm:

It was developed by two German researchers, Pfitzmann and Westfield, in order to eliminate the security issue that arises when data is embedded in a JPEG image, in which the message is embedded in a randomly selected Discrete Courier Transform (DCT) parameter. It uses an inclusion matrix that minimizes changes in message length. This algorithm provides high hiding capacity prevents optical attacks and is resistant to statistical attacks, as it does not replace bits. It has an embedding capacity higher than 13%, and supports TIFF, BMP, JPEG and GIF image formats.

C. LSB (Least Significant Bit Algorithm):

Least Significant Bit Substitution (LSB) is a basic method of embedding a message within a picture by changing the pixels' Least Significant Bit. The length of the message entered in LSB varies depending on the number of image bits, for example an 8-bit image, the eighth broadcast of each image pixel is changed by bits from the secret message. But if the image is 24-bit, the colors of each RGB point (red, green, blue) are changed, as the eighth broadcast of each color is changed by a bit of the secret message, as shown in Figure (7). LSB is effective when using BMP images as BMP images have less lossy compression. But the LSB algorithm needs a large image to be used as a cover. LSB replacement can be used on GIFs as well, but the problem is that in GIF, whenever LSB is changed the whole color changes, and this problem can be avoided only by using GIFs that are gray scale and have 256 shades and the changes will be gradual so it will be difficult to detect. As for JPEG images, they cannot be used with direct-replacement masking techniques, as they will use lossy compression.
The effectiveness and performance of the above algorithms varies depending on the type of cover image or the source in which the data is contained**.**

D. Digital Watermarking:

"It is a process that hides the watermark data in a Multimedia Object so that the watermark can be observed and distinguished from the data of the object to assert its ownership or verify its integrity" (Stallings, 2013). Watermarking techniques are divided into two categories: robust watermark and delicate watermark. Because of its power against all types of image modifications, solid watermarks are mostly utilized for copyright protection. The second category (fragile) is utilized to provide increased reliability and integrity checks in order to prevent unauthorized modifications.

3.11 Ninthly: Stages of designing systems to embed text in the image:

The text Steganography system is based on three basic stages as follows:

A. Embedding Phase:

This stage uses two types of files to perform the hiding process, the first is the secret data to be sent secretly, and the other is the carrier file, which is an image file, in which the data after encrypting is included in the image using the LSB algorithm, which replaces the least significant bit of the file points the image is in bits of the transmitted data. That is, the encoded data bits are combined with the bits of the carrier file, resulting in the cover image. With this procedure, the LSB algorithm helps to secure the image's originality and preserve its purity.

B. Transmission Phase:

The data is sent to the target securely because the hiding stage results in the image covering the embedded or hidden data, and this image is secured with a secret key, and e-mail or the web is usually used to send the data. About the text and making unauthorized modifications.

C. Extraction Phase:

It is the opposite of the hiding stage, in which the image carrying data (the cover image) is used as input, and the same password is used in the cloaking to protect the data from unauthorized access. After entering the proper password, the retrieval stage employs the LSB algorithm, which returns the image's bits in order to extract the contents.

3.12 Eleventh: The procedure for hiding data in the proposed system:

A. Firstly, the sender uses an invisibility app to hide the text inside the image after it has been encrypted.
B. For encryption, the text to be hidden is written, then the sender uploads the image in which the text is to be hidden, then the password in the space designated for them.
C. The sender presses hide and from here the encryption process begins using the Rijndael algorithm which is the encryption of the password and the production of a key used to encrypt the text to eventually result in the encrypted message.
D. The program hides the encrypted message in the image using the LSB algorithm to produce the cover image. The stages of the hiding process can be summarized in the following points:

- Read the cover file and read the file to be hidden.
- Convert the file to be hidden to binary format.
- Calculate the least significant bit in a cover file by bits from the file to be hidden one by one.
- Save the output in a new file with the same cover type as the original (image, audio, or video).
- The program alerts the sender of the end of the hiding process and allows him to store it in an image file of his choice.

The image is sent to the target or recipient through a transmission medium such as the Internet or a local network using e-mail, one of the chat applications available on the Internet, or storage media such as flash and optical disc.
g. The decoding stage begins with the message being received by the recipient, who uses the program to download the received image file and enter the password to retrieve the text.
h. The recipient presses retrieve so that the program begins the process of retrieving the message, decrypting it, and displaying it to the recipient. The retrieval process can be summarized in the following points:

- Undo the cover file.
- Calculate and select the least significant bit in the cover file.
- Retrieve the least significant bit in the cover file.
- Convert the bit set to its numeric form (in the case of text, for example, every 8 bits are converted to a character, and so on).

3.13 Twelfth: Experimentation:

The performance evaluation process that was carried out in this research was based on conducting several empirical tests to verify that the transmitted data was not observed and to ensure the performance of the proposed system. The evaluation was made based on visual observation by comparing the cover image before hiding the secret message in it with the same image after the concealment process. By experimenting with different images and different messages, it became clear that the human eye cannot perceive the difference between the images and the histogram of images before and after concealment.

3.14 Thirteenth: Conclusions:

It is important to protect data in the digital world; this is due to the increase in security threats due to the significant expansion in the use of digital means of communication in the exchange of data. Through this research and the experiments conducted on the proposed system, the two researchers reached the following results:
A. Secret messages can be encrypted and hidden inside color images to protect them from hacking and retrieve them in a way that ensures their safety.
B. The human eye cannot perceive the presence of a hidden text message inside the sent image, because the system can

combine them, so that there is no risk of sending them through an insecure channel. Therefore, it is difficult to obtain information by unauthorized persons.
C. The inability of the naked eye to have a difference in the image histogram before and after merging increases the efficiency and robustness of the proposed system.
D. Even if the data hackers somehow manage to find out that there is a hidden message inside the image, it is difficult for them to read the message because it is encrypted with a password.

References:

[1] Hasso, Shahd. Hiding compressed texts in an audio file, Al-Rafidain Journal of Computer Science and Mathematics, Volume (10) Issue (1), (a special issue of the proceedings of the Fifth Scientific Conference in Information Technology). - 2013.

[2] Kandilji, Amer Ibrahim et al. Information and Communication Networks, Amman: Dar Al Masirah, 2012.

[3] Hussein, Abdul Amir Khalaf. Encryption Methods for Beginners, Amman: Dar Wael for Publishing and Distribution, 2010.

[4] Al-Hamami, Alaa Hussein and Al-Ani, Saad Abdel-Aziz. Information Security Technology and Protection Systems, Amman: Dar Wael for Publishing and Distribution, 2007.

[5] Abdullah Sadoon Hussein, Steganography Methods and some application (The hidden Secret data in Image) , Mosul : University of Mosul, 2009.

[6] Andrews Chinchu Elza and Joseph Iwin Thanakumar, An analysis of various stegnographic algoritms, International Journal of Advanced Research in Electronics and Communication Engineering (IJAREC) .Volume 2, Issue 2, February 2013.

[7] Felicisimo V. W., Bobby D. G. and Bartolome T. T. Modified AES Algorithm using Multiple S-Boxes". Proceedings of the Second International Conference on Electrical, Electronics, Computer Engineering and their Applications (EECEA) , Manila, Philippine, 2015.

[8] Fouad Mohamed M, Enhancing the Imperceptibility of Image Steganography for Information, The Federated Conference on Computer Science and Information Systems, 2017. - pp. pp. 545–548.

[9] Jeffrey A Bloom, Digital watermarking and steganography, Morgan Kaufmann publications, 2008.

[10] Joye M., Cryptographic Hardware and Embedded Systems-CHES, New York, 2004.

[11] Kevin L., Advanced Encryption Standard (AES) Selection Process- How Rijndael Won, MIDN 1, 2015.

[12] Kobayashi L, Furuie S and Barreto P, Providing Integrity and Authenticity in DICOM Images: A novel Approach, IEEE Transactions on Information Technology in Biomedicine. - 2009. - pp. pp. 582-589.

[13] Koduri Nani, Information Security through Image Steganography Using Least Significant Bit Algorithm, London: University of East London, 2011.

[14] Stallings W., Cryptography and Network Security: Principles and Practice : Prentice Hall, 2013.

[15] Sumathy V. and Navaneethan C., Enhanced AES Algorithm for Strong Encryption, International Journal of Advances in Engineering& Technology (IJAET). - 2012.

[16] Whitman M E and Mattord H J, Principles of information security, Thomson, 2012.

[17] Zinaly Elham and Naghipour Avaz, Audio Steganography to Protect the Confidential Information: A Survey, International Journal of Computer Applications. - July 2017. - pp. 22-29.

Sameer A. Nooh received the BSc. A degree in Computer Science from King Abdulaziz University, Jeddah, Saudi Arabia, and MSc Internet, Computer and System Security from University of Bradford, UK in Information Security in 2007. MSc consultancy from Liverpool John Moores University. Sameer finished his Ph.D. in Computer Science De Montfort University in Leicester, UK 2014. In 2015, Dr.Sameer joined the Computer Science Department, University of Tabuk, as an Assistant Professor in the Computer Science Department, University College, Umluj. His main areas of research interest are Information and System Security, Computer Science, and anything related to the Internet and computer. Since 2014 Dr. Sameer started some administrative assignments includes: Supervisor of Information Technology Unit, Vice-dean of University College, Umluj and now he is Dean of University College, Umluj, University of Tabuk, The northern area, Tabuk, Saudi Arabia.