Combination of Steganography and Cryptography: A short Survey

Mustafa Sabah Taha\textsuperscript{1,3}, Mohd Shafry Mohd Rahim\textsuperscript{1,2}, Sameer abdulsattar lafta\textsuperscript{4}, Mohammed Mahdi Hashim\textsuperscript{1,5}, Hassanain Mahdi Alzuabidi\textsuperscript{6}

\textsuperscript{1}School of Computing, Facility of Engineering, University Technology Malaysia, Johor Bahru, Malaysia
\textsuperscript{2}UTM (IRDA) Digital Media Center, Faculty of Computing, University Technology Malaysia, Johor Bahru, Malaysia
\textsuperscript{3}Basrah Oil Training Institute, Ministry of Oil, Iraq
\textsuperscript{4}Technical Instructors Training Institute, Middle Technical University, Baghdad, Iraq
\textsuperscript{5}Faculty of Engineering, Uruk University, Baghdad, Iraq
\textsuperscript{6}Ferdowsi University of Mashhad Faculty of Engineering Computer Engineering Department

Abstract. The establishment of a secure communication between two communicating parties is becoming a difficult problem due to the likelihood of attacks and other unintentional changes during an active communication over an unsecured network. However, the security of secret information can be secured using either cryptography or steganography. Steganography refers to the practice of concealing a message (with no traceability) in a manner that it will make no meaning to anyone else except the intended recipient, while cryptography, on the other hand, refers to the art of converting a plaintext (message) into an unreadable format. Thus, steganography conceals the existence of a secret message while cryptography alters the message format itself. Both steganographic and cryptographic techniques are powerful and robust. In this paper, the major aim is to review several ways of combining steganographic and cryptographic techniques to achieve a hybrid system. Moreover, some of the differences between cryptographic and steganographic techniques were presented as well.

Keywords: Information hiding, Cryptography, Image steganography, Security, Image quality.

1. Introduction
It is true that the emergence of the Internet and its subsequent expansion has made digital communication easier, but with additional cost and that is the issue of information security over open networks. Sending and receiving information via email or the use of web browsers are not secure as sensitive information such as credit card information sent over such medium can be intercepted [1]. There is a need for a private and secure communication for online users. To solve the issue of information threats, several methods (Table 1) have been proposed in the area of systems security under information hiding and encryption [2].
Table 1. Basic security system classification [2]

| Security System | Information Encryption | Cryptography | Public Cryptography |
|-----------------|------------------------|--------------|--------------------|
|                 |                        | Steganography| Linguistic Steganography |
|                 |                        | Watermarking | Technical Steganography |
|                 |                        |              | Robust Watermarking |
|                 |                        |              | Fragile Watermarking |

Cryptography is also referred to as information encryption while steganography is also called information hiding. These are the most significant techniques for information security [3]. With cryptography, the secret information is altered in a way that it cannot be readable to eavesdroppers, but with steganography, the existence of the secret information is completely concealed from unauthorized persons [4-5].

The value of the confidential data obtained from a system is the most important thing to the attacker [6,7]. The data may be compromised, distorted, or even deployed for future attacks by attacker [8]. A perfect way of solving these problems would be to exploit the advantage of cryptographic and steganographic techniques to develop a hybrid system which can be stronger than the individual strengths of the component techniques. In this paper, section 2 presented a historical background about cryptographic and steganographic techniques, with emphasis on the basic differences between them, while section 3 reviewed the methods of combining steganographic and cryptographic techniques. Section 4 presented the conclusions of the review.

2. Background

Steganography and cryptography are two different techniques that maintain data confidentiality and integrity [9]. The purpose of steganography is to hide secret messages in digital media in a way that does not allow anyone to detect the existence of such secret messages [10]. The main purpose of steganography is to communicate securely with secret messages through pictures [11]. Steganography does not change the structure of the secret message, but it hides inside the media so the change is not visible [11]. While cryptography protects messages from unauthorized individuals by changing their meaning [12]. Steganography techniques depend on the confidentiality of the data encoding system [13] once the encoding system is known, the steganography system can be known or tracked. The stenographic technique enables the concealment of the fact that messages are being transmitted through digital media, such communication techniques are invisible between the sender and the receiver [14], while cryptography obscures the integrity of the information so that it is not understood by anyone but the sender and receiver [9]. Cryptography is a mathematical study that has links to aspects of information security such as data integrity, entity authenticity and data authenticity [15]. However, there is a need to provide further clarification of these techniques to assist in the understanding of the advantages of their combination.

2.1 Cryptography

Cryptography refers to the act of secret writing through the enciphering and deciphering of encoded messages [9]. It is evidenced in situations where communication is established between two parties over an insecure medium which can be easily eavesdropped (Figure 1).
Gollmann [16] described cryptography as a pool of cryptographic techniques comprising encryption and decryption frameworks, integrity, check functions, and digital signature frameworks. Encryption frameworks are used to alter secret messages into illegible formats to an unauthorized person while decryption frameworks are used to decode the scrambled message by a person who is authorized to do so. A cryptographic hash function is an example of an integrity check function [17]. It is a mathematical relation used to identify small pieces of information which can be used to specifically identify larger digital objects. There are different hash values for different objects; thus, it is not computationally possible to have an object with the same hash value as that of an existing object [18]. Hash functions serve as a yardstick for the verification of the integrity of a message after transmission. Another form of integrity check function is the message authentication codes (MACs) [19], which are derived from two inputs - the transmitted message and the cryptographic secret key. It is also used to check for the integrity of a message post-transmission. Digital signature algorithms used for the detection of message alteration by an invader during an active communication. It is based on the same principles as asymmetric encryption [20].

2.1.1. Uses of cryptography
The encryption aspect of cryptography is mainly for the protection of sensitive information unsolicited alterations. It involves the encryption of the stored data information and encryption of the information to ensure a secure communication [21-23]. If an encrypted message is successfully intercepted by an eavesdropper, it will be useless to the attacker because an encrypted message cannot be possibly decrypted by an authorized person.

2.1.2. Encryption algorithms and the cryptographic key
The first principles of cryptographic engineering were formulated by Auguste Kerckhoff in 1883 [24]. This principle states that an encryption technique may be publicly known but the decryption of the message requires knowledge of the key [24]. This key is deployed at both the encryption and decryption phases, and without it, it is not possible to decrypt an encrypted message even if the encryption algorithm is known. The modern encryption frameworks are broadly classified into two groups which are symmetric and asymmetric encryption algorithms. This classification is based on the role of the keys in each algorithm. The symmetric encryption algorithms (SEA), also called secret-key encryption (SKE) require both the message sender and the receiver to be in possession of a common secret key for encrypting and decrypting the message (Figure 2).
The asymmetric encryption algorithms (AES), also called public key encryption (PKE), require both the message sender and the receiver to two keys in which one key is available to the public while the other is a private one (Figure 3). Both encryption techniques ensure the security of information against communication vulnerabilities over an insecure medium [25].

![Figure 2. A basic pictorial of symmetric encryption](image)

Figure 2. A basic pictorial of symmetric encryption

The asymmetric encryption algorithms (AES), also called public key encryption (PKE), require both the message sender and the receiver to two keys in which one key is available to the public while the other is a private one (Figure 3). Both encryption techniques ensure the security of information against communication vulnerabilities over an insecure medium [25].

2.1.3. Security services offered by cryptography

Message confidentiality is the fundamental security service guaranteed by cryptographic techniques. It is achieved by using encryption algorithms. Both SEA and AES make use of private keys to ensure data privacy [26]. However, both techniques depend on the length of the secret keys to guarantee information security. Having sent a message, the sender and the receiver of the message need to verify the integrity of the message during the transmission process using the cryptographic hash functions. Note that a message can be intentionally or unintentionally altered during transmission [24]. The authenticity of messages can also be ensured through digital signature schemes [27] or support non-repudiation. The digital encryption schemes are based on the same principles as the AES; they encrypt messages with a private key with the encrypted message acting as a signature since it could only be decrypted using a specific private key. The security services attributed to cryptography by the ISO 7498-2 include confidentiality, data integrity, identification, authentication, and non-repudiation.

2.1.4. Encryption problems

Regarding different encryption algorithms, a notable issue with the SEA is the possibility of compromising the information if the key is stolen. Hence, this leads to another problem which is the secure distribution of keys [18]. The encryption key can either be exchanged face-to-face by the parties, sent through a trusted courier, or transmitted through an existing cryptographically secure channel. The first methods are not unsafe while the third choice depends on the experience from the previous key exchange. A secure key distribution is not enough; the keys must be stored, used, and destroyed securely as well. The problem of key distribution is solved by the public key encryption method deployed in the AES but it has its own problems. The public encryption key relies on a mathematical function which is yet to be proven unsolvable [28]. Currently, there is no algorithm which can quickly establish the mathematical relationship between the public and the private keys such that one can be used to uncover the other; however, such a system cannot be ruled out. The development of such a system will compromise the encryption method and make the algorithm vulnerable [28]. As per Gollmann [16], cryptography rarely offers a solution to security problems but often a way of transforming a problem into another form. The implementation of cryptography in security systems only succeeds in converting the problem from a secure communication problem into
another of key management. This is often the case with the intention that it will yield a better solution than solving the original version of the problem. The drawbacks of cryptography are summarized as key distribution problem, mathematical vulnerabilities of asymmetric encryption, legal limitations by governments, and cryptanalysis.

2.2. Steganography
Steganography refers to the ways of concealing a secret message into a cover message in a manner that its existence is completely hidden [29-31]. The secret message can be in the form of a plaintext, an image, a cipher text, or anything which can be represented as a bit [24]. Sometimes, the embedding process is parameterized by a stego-key (secret key) which must be known before the secret message can be detected and extracted. Once a message is hidden in a cover message, it is referred to as a stego-object. Figure 4. depicts a general steganographic model. Before embedding an information in a cover, the sender must first transform the secret message, then manipulate some of the bits of the cover object to form the stego-object [32,33]. Then, the stego-object is transmitted over a communication medium to the intended receiver. When received, the process is performed in a reverse manner to extract the hidden info. If the process involves a secret key, both parties (sender and receiver) must have the key prior to the transmission of the stego-object [34].

![Figure 4. Main diagram of steganography](image)

Watermarking and fingerprinting are the two other techniques that are related to steganography, but they are not in the same class [35] as they mainly ensure the protection of intellectual property. Thus, watermarking, fingerprinting, and steganography differs in robustness, application and hiding capacity [36].

2.2.1. Uses of steganography
Steganography is generally used in the communication of secret and when total freedom is desired. Communication security is very important in both censured and monitored surroundings. Private communications which cannot be secured through cryptography can be secured with steganography [37]. However, Conklin [38] suggested the use of steganography with other security mechanisms for the provision of layered security as an intruder who succeeds at one layer is still required to bypass the other levels to be completely successful. Communications in the military and intelligence fields...
require no obstruction; even with content encryption, the detection of a signal can result in an attack on the sender on a modern battlefield [39]. Such signals can be hidden through steganography. Information that is not intended to be shared with anyone can also be stored using steganography. Other sensitive information such as banking information can also be concealed in a cover object and stored on a private computer [40,41].

2.2.2. Steganography algorithms and the steganographic key
Different steganographic algorithms have been deployed to ensure data security. It should be noted that not all steganography systems operate with secret keys; however, the security of steganographic systems can be enhanced by applying the Kerckhoff principle. The principle implies that even if an intruder knows the design and implementation of the steganographic system, he must have the secret key to launch a successful attack on the system. Therefore, it may be wise to incorporate the secret keys (public or private) when implementing steganographic systems [24].

2.2.3 Security services offered by steganography
Steganography provides sensitive information security through the embedding of the information in another information; thus, there is confidentiality. Such hidden information can only be revealed using a steganographic key [37]. However, the technique and manner used to conceal the information could also serve as identity proofs. The technique for embedding the information, can become a shared secret if wrongly done, can be a mode of identification and authentication [24]. The embedded information cannot be subjected to integrity check because the information may have been altered intentionally or unintentionally, and the changes made to the extracted information may not be observed [42].

2.2.4. Steganography problems
Computer scientists and security analysts have recently recognized the security threats posed by the illicit use of steganographic techniques in the global information space [43]. Terrorists can utilize steganography to communicate secretly without the knowledge of the law enforcement agencies. Owing to this, studies have been on going to find the problems of the existing steganographic systems which can be exploited for hidden information detection, extraction, and/or destruction. There are two major techniques in steganalysis; visual analysis and statistical analysis. The aim of visual analysis is to reveal the presence of hidden information through a naked eye or computer-aided inspection. Statistical analysis tries to reveal small alterations in the carrier objects (it tries to unravel the statistical features associated with steganographic processes) [44]. Furthermore, secret information can be removed by email firewall when filtering images and this is another threat to image steganography. However, most of the proposed image steganographic techniques do not rely on e-mail as a communication channel, rather, on websites which can also distribute stego images. [43].

2.3. Cryptography versus Steganography
To propose steganography as an alternative to cryptography, it requires a comparison between the two techniques. Table 2 presents a summary of the two techniques in terms of their security services, applications, problems, robustness and other criteria.
Table 2. A comparative analysis of Encryption and Steganography

| Criteria/Method         | Encryption | Steganography               |
|-------------------------|------------|-----------------------------|
| Objective               | Data protection | Secret communication        |
| Input                   | One        | At least two                |
| Output                  | Cipher text | Stego file                  |
| Key                     | Necessary  | Optional                    |
| Carrier                 | Usually text | Text, Message, Audio, Video, Protocol and DNA |
| Security Service        | Authentication, Confidentiality, Identification, Data Integrity and Nonrepudiation | Authentication, Confidentiality, Identification |
| Visibility              | Always     | Never                       |
| Type of attacks         | Cryptanalysis | Steganalysis                |
| Attacks                 | Broken when attacker can understand the secret message, known as Cryptanalysis | Broken when attacker reveals that steganography has been used, known as Steganalysis |
| Naked eye identification| Yes, The secret message will convert in another way. | No, The secret message will hide within the cover image (Carrier). |
| Fails                   | de-ciphered | When it is detected payload |
| Secret data             | Plaintext  | Information security        |
| Applications            | Information security | Information security |
| Technology-specific problems | Key distribution | Key distribution (except with keyless) |

3. Combining Cryptography and Steganography

Steganography and cryptography have been noted to be individually insufficient for complete information security; therefore, a more reliable and strong mechanism can be achieved by combining both techniques [45]. Combining these strategies can ensure an improved secret information security and will meet the requirements for security and robustness for transmitting important information over open channels. Figure 5 presents a strategy for the combination of both techniques.

![Figure 5. Basic diagram of combining steganography and cryptography](image)

3.1 Literature review

As earlier stated, information security is gaining more attention due to the increase in the size of data being transferred over the Internet. One of the proposed solutions is the exploitation of the advantages of cryptographic and steganographic techniques through their combination into a hybrid technique.
The method for this combination has been proposed in many studies although previous reviews have failed to properly address them.

The combination of many steganographic techniques with different algorithms such as cryptography, AES algorithm, random key generation, alteration component, and key-based security algorithms has been reviewed [46]. The number of reported threats to data security is continuing to increase in the past few years and is becoming a serious security challenge. These threats can be best nullified using cryptographic and steganographic techniques. Current studies suggest the combination of both techniques to achieve a more robust and stronger framework with a better security compared to the individual components.

An encrypting technique based on the combination of cryptographic and steganographic techniques for embedding data was proposed by Dhamija, A., & Dhaka, V [47]. For the cryptographic aspect, they proposed the use of SCMACS which is an effective data encryption technique that uses one’s complement method. It uses a symmetric key approach in which both the message sender and the recipient share the same encryption and decryption key. For the steganographic aspect, they proposed the use of the mostly preferred LSB method.

A highly-secured steganography technique comprised of a combination of DNA sequence with Hyperelliptic Curve Cryptography was proposed [48]. This approach prides the advantages of the component techniques to ensure a higher level of communication security. To conceal a secret message using this algorithm, the image is first converted into DNA sequences using the nucleotide to a binary transformation table. There are three steps from the side of the sender in this algorithm; first, the pixel values of both the secret message and the cover image must be converted to their respective DNA triplet value using characters to the DNA triplet conversion; then, the triplet values will be converted to the binary values form. The final stage involves the application of XOR logic on the secret and cover images’ binary values to generate the stego image.

Another study presented a multi-level secret data embedding technique comprised of integrated visual cryptography and steganography [49]. Here, a method known as halftoning was used to reduce image pixels and make the processing step easy. After that, a visual cryptographic technique is applied to produce the shares (forming the first level of security) before applying an LSB-based steganographic technique to conceal the shares in different cover images.

The combination of a strong encrypting scheme and steganographic technique was proposed to ensure the safety of confidential message during transmission [50]. This method proposed the use of AES-128 key encryption technique to first encrypt the secret message before its encoding into a QR code. Then, the encrypted message in the UTF-8 format is converted into base 64-format to ensure it is compatible for further processing. Then, another level of security is added to the process by scrambling the encoded image. Finally, the scrambled QR code is hidden in a suitable carrier which is securely transmitted to deliver the hidden information. the method adopted a least significant bit method to achieve the digital image steganography. When the message is received by the recipient, the secret data is extracted from the carrier through a decoding process, meaning that a four-level security can be achieved with this method during the transmission of a secret message.

An image steganography method which utilized the DES algorithm for text message encryption was presented [51]. The method uses a 16 round and block size 64-bit. Later, the K-means pixel clustering method was used to clusters the image into several segments and embed the data in each segment. Several clustering algorithms was used for image segmentation. Segmentation comprised of a large set of information presented in the form of pixels; each pixel further has three components which are Red, Green, and Blue (RGB). Having formed the clusters, they used an LSB method to partition the encrypted message into K number of segments which are to be concealed in each cluster.

Cryptography and steganography alone have been reported to be inadequate for the transmission of data due to their inherent weaknesses [52]; hence, a system based on the two technologies was proposed in which it will be almost impossible for a third party to breach the security of the system and extracts confidential information. In the proposed system, a recently developed Two Fish algorithm was used for the encryption process while an Adaptive B45 steganography technique was used for the steganography.
A method for the extension of the embedding capacity and enhancement of the stego image quality was proposed [53]. This method used the Adaptive Pixel Value Differencing method for the steganographic processes while AES was relied upon for the cryptographic aspect. This method used an image as the carrier to embed secret data. This carrier image must be a grayscale image; hence, the pixel size should be about 256 x 256. Pixels of higher sizes were trimmed to this range, and color cover images are changed into grayscale images before usage. The data was embedded into the cover image using an APVD algorithm. The achieved stego image was encrypted using an AES algorithm.

A performance analysis survey has been conducted on several algorithms such as DES, AES, and RSA in combination with the LSB substitution technique [54]. The analysis shed light on the three encryption algorithms in any application based on their performance. The work concluded that AES was better than DES and RSA as it used a less buffer space and offered less encryption and decryption times.

A modern method which is based on the Huffman encoding method to hide data was presented by (names) [55]. Here, the cover image was a gray level image of size m x n while the secret image was of size p x q. After that, the Huffman encoding process was executed on the secret image and an LSB algorithm was used to embed each bit of Huffman code of the secret image into a cover image.

A new steganographic technique which depends on a secret key, cryptography and image transposition to perform a gray-level modification for true color images was proposed by (names) [56]. Here, multiple encryption algorithms are first used to encrypt both the secret information and the secret key before embedding them in a cover image. In addition, the input image is changed prior to the embedding process. The proposed method offers five levels of security through image transposition, bit-XORring, bits shuffling, stego key-based encryption, and gray-level modification. This makes the data recovery a difficult job for attackers.

An approach which deploys Blowfish encryption for secret information encryption prior to LSB-based embedding was proposed by [57], while [58] used AES algorithm to encrypt secret data and prevented external attacks using SHA-1. Later, they encrypted the image information using an LSB method. To recover the message, the recipient must use the hash that is provided by the sender. Different types of media can be used to hide the secret data, providing more levels of security.

The hiding of secret information using steganographic and cryptographic techniques was discussed by [59]. They proposed a new method which can secure data without altering the quality of an image as a carrier. They used the steganographic method to find the message bits that matched the most significant bit of the image cover. A divide and conquer approach was used to find this similarity. The matching outcomes were the bit index position which they later used the DES method to encrypt.

A new method in which the secret message is first transformed into ciphertext using an RSA algorithm was proposed by [60]. In the next step, the ciphertext is embedded in an audio using the LSB audio steganographic technique. The recipient of the message must first extract the ciphertext from audio before using RSA decryption algorithm to decrypt the message. Therefore, this technique boosts the combined characteristic of cryptographic and steganographic techniques and offers a higher level of information security.

The Blowfish cryptography algorithm was used by [61] for secret image encryption. The Blowfish was used because it is stronger and faster, and provides a good performance compared to some other algorithms like RC6, RC4, DES, 3DES, and AES. Here, the secret image was selected in a BMP format and encrypted using the Blowfish algorithm. Next, the encrypted image was embedded into video frames using LSB embedding method. This method provides information authenticity, confidentiality, integrity, and non-repudiation.

A similar technique was also provided by (names) [62] but the difference here is that text was used as a secret message rather than an image as in [61] and encrypted using a Blowfish algorithm. Next, an image was used as a cover object while an LSB technique was used to embed the encrypted text into this cover.

A new method which used an RSA algorithm with a 128-byte key size for secret information encryption prior to embedding in a cover image using an F5 steganographic algorithm was proposed by [63]. They randomly used DCT coefficients to embed the secret data into the cover using the F5 algorithm. A matrix embedding technique was applied to minimize the alterations in the length of a
specific message, thereby giving a faster speed, high steganographic ability, and security from observed and analytical attacks.

A novel visual cryptographic technique which is suitable for both Bitmap color and Grayscale images was proposed by [64]. The method used the Residual Number System theory which is based on the Chinese Remainder Theorem for share creation and shares stacking of a given image. The secret image was first embedded in a cover image to create the stego-image; then, an 8-bit pixel stego-image and an 8-bit key were combined to produce a cipher pixel using an additive mod 255 algorithm. The key was generated using a pseudo-random number generator and a mixed key generation method. After encrypting the stego image, they cipher pixel was mapped into a Residue Number System of n pieces before finally collecting and sending n pieces to the recipient. This is an extremely fast, secure, efficient, easy to implement, and reliable approach.

A combination of cryptographic and steganographic techniques was proposed by [65], in which an AES algorithm was combined with an LSB algorithm. The LSB technique was used to embed the secret data into an image file while the AES algorithm was used to encrypt the generated stego image. The study suggested this technique as an effective method for transmitting secret information with a better level of security.

A comparative study of steganography and cryptography was performed by Almuhammadi et al. [66]. They surveyed several methods of combining cryptographic and steganographic techniques in one system. Moreover, they presented a classification of these methods and compared them in terms of the algorithms used for encryption, the steganographic technique used, and the file type used as a cover. Consequently, they concluded that the methods which start with cryptography were more common than methods which start with steganography and provided better security with less encrypted data exposure. The only advantage of methods which start with steganography was providing more capacity for the secret information.

4. Conclusions

After making a comparison study between the science of Cryptography and Steganography, the authors cannot guarantee that steganography can be used as an alternate to Cryptography as each aspect has its peculiarities.; Cryptography refers to the act of secret writing through the enciphering and deciphering of encoded messages, while Steganography refers to the ways of concealing a secret message into a cover message in a manner that its existence is completely hidden. Using only one of these techniques will render the system vulnerable to the third party. Therefore, the combination of Steganography and Cryptography give more security and robustness.

References

[1] Almuhammadi S and Al-Shaaby A 2017 A survey on recent approaches combining cryptography and steganography Computer Science Information Technology (CS IT).
[2] Cheddad A, Condell J, Curran K, Mc Kevitt P 2010 Digital image steganography: Survey and analysis of current methods Signal processing 90 727-752.
[3] Moody G D, Siponen M and Pahnila S 2018 Toward a unified model of information security policy compliance MIS Quarterly 42 1.
[4] Acar A, Aksu H, Uluagac A S and Conti M 2018 A survey on homomorphic encryption schemes: theory and implementation ACM Computing Surveys (CSUR) 51 79.
[5] Hashim M, Rahim M, Shafry M and Alwan A A 2018 A review and open issues of multifarious image steganography techniques in spatial domain Journal of Theoretical & Applied Information Technology 96.
[6] Diesburg S M and Wang A I A 2010 A survey of confidential data storage and deletion methods ACM Computing Surveys (CSUR) 43 2.
[7] Matthews G J and Harel O 2011 Data confidentiality: A review of methods for statistical disclosure limitation and methods for assessing privacy Statistics Surveys 5 1-29.
[8] Seth D, Ramanathan L and Pandey A 2010 Security enhancement: Combining cryptography and steganography International Journal of Computer Applications 3-6.
[9] Joseph A and Sundaram V 2011 Cryptography and steganography–A survey.
[10] Laskar S A and Hemachandran K 2012 Combining JPEG steganography and substitution encryption for secure data communication *Computer Science & Information Technology (CS&IT)*.

[11] Johnson N F and Jajodia S 1998 Exploring steganography: Seeing the unseen *Computer 31*.

[12] Katz J, Menezes A J, Van Oorschot P C and Vanstone S A 1996 *Handbook of applied cryptography* CRC press.

[13] Conway M 2003 *Code wars: steganography, signals intelligence, and terrorism* Knowledge, Technology & Policy 16 45-62.

[14] Walia E, Jain P and Navdeep N 2010 An analysis of LSB & DCT based steganography *Global Journal of Computer Science and Technology*.

[15] Zaidan B B, Zaidan A A, Al-Frajat A K and Jalab H A 2010 On the differences between hiding information and cryptography techniques: An overview *Journal of Applied Sciences (Faisalabad)* 10 1650-1655.

[16] Gollmann D 2010 Computer security *Wiley Interdisciplinary Reviews: Computational Statistics* 2 544-554

[17] Saint-Andre P, Wild M, Smith K and Markmann T 2018 Use of Cryptographic Hash Functions in XMPP.

[18] Jallad K, Katz J and Schneier B 2002 September Implementation of chosen-ciphertext attacks against PGP and GnuPG *In International Conference on Information Security* (pp. 90-101) Springer, Berlin, Heidelberg.

[19] Yadav H 2018 Secure Multi-party Communication with Verifiable Outsourced Decryption for Mobile Cloud Computing.

[20] Lyubashevsky V, Micciancio D 2018 Asymptotically Efficient Lattice-Based Digital Signatures *Journal of Cryptology* 1-24.

[21] Goorden S A, Horstmann M, Mosk A P, Škorić B and Pinkse P W Quantum-secure authentication of a physical unclonable key: supplementary material *Quantum* 9 10.

[22] Mitali V K and Sharma A 2014 A survey on various cryptography techniques *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)* 3 307-312.

[23] Jirwan N, Singh A and Vijay D S 2013 Review and analysis of cryptography techniques *International Journal of Scientific & Engineering Research* 4 1-6.

[24] Morkel T 2012 Image steganography applications for secure communication *Doctoral dissertation*, University of Pretoria.

[25] Patarin J 1996, August Asymmetric cryptography with a hidden monomial *In Annual International Cryptology Conference* (pp. 45-60) Springer, Berlin, Heidelberg.

[26] Yassein M B, Aljawarneh S, Qawasmeh E, Mardini W and Khamaysah Y 2017, August Comprehensive study of symmetric key and asymmetric key encryption algorithms. *In Engineering and Technology (ICET), 2017 International Conference on* (pp. 1-7) IEEE.

[27] Hoffstein J, Schanck J M, Silverman J H and Whyte W J 2017 *U.S. Patent No. 9,634,840*. Washington, DC: U.S. Patent and Trademark Office

[28] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Quantum cryptography *Reviews of modern physics* 74 145.

[29] Hashim M M, Rahim M S M, Johi F A, Taha M S, Al-Wan A A and Sjarif N N A 2018 An extensive analysis and conduct comparative based on statistical attack of LSB substitution and LSB matching *International Journal of Engineering & Technology* 7 4008-4023.

[30] Douglas M, Bailey K, Leeney M and Curran K 2018 An overview of steganography techniques applied to the protection of biometric data *Multimedia Tools and Applications* 77 17333-17373.

[31] Mishra S, Yadav V K, Trivedi M C and Shrimlai T 2018 Audio Steganography Techniques: A Survey *In Advances in Computer and Computational Sciences* (pp. 581-589) Springer, Singapore.

[32] Petitcolas F A, Anderson R J and Kuhn M G 1999 Information hiding—a survey *Proceedings of the IEEE* 87 1062-1078.
[33] Cao Y, Wang Y, Zhao X, Zhu M and Xu Z 2018, June Cover Block Decoupling for Content-Adaptive H. 264 Steganography In Proceedings of the 6th ACM Workshop on Information Hiding and Multimedia Security (pp. 23-30) ACM.

[34] Al-Husainy M A F and Uliyan D M 2018 Image Steganography Technique Based on Extracted Chains from the Secret Key Journal of Engineering and Applied Sciences 13 4235-4244.

[35] Petitcolas F A, Anderson R J and Kuhn M G 1999 Information hiding-a survey Proceedings of the IEEE 87 1062-1078.

[36] Wang H and Wang S 2004 Cyber warfare: steganography vs. steganalysis Communications of the ACM 47 76-82.

[37] AL-Shaaby T 2017 Cryptography and Steganography: New Approach Transactions on Networks and Communications 5 No. 6.

[38] Conklin W A, White G, Cothren C, Davis R and Williams D 2015 Principles of computer security McGraw-Hill Education Group.

[39] Khanam M S, Verma M J A 2018 Novel And Efficient Video Steganography Approach for Enhanced Security.

[40] Devadiga N, Kothari H, Jain H and Sankhe S 2017 E-Banking Security using Cryptography, Steganography and Data Mining International Journal of Computer Applications 164 9.

[41] Hashim, M, Rahim M, Shafry M and Alwan A A 2018 A review and open issues of multifarious image steganography techniques in spatial domain Journal of Theoretical & Applied Information Technology 96 4.

[42] Domain W T I S 2018 A review and open issues of diverse text watermarking techniques in spatial domain Journal of Theoretical and Applied Information Technology 96 17.

[43] Siper A, Farley R and Lombardo C 2005 The rise of steganography Proceedings of Student/Faculty Research Day CSIS, Pace University.

[44] Hussain M, Wahab A W A, Idris Y I B, Ho A T and Jung K H 2018 Image steganography in spatial domain: A survey Signal Processing: Image Communication 65 46-66.

[45] Aung P P and Naing T M 2014 A novel secure combination technique of steganography and cryptography International Journal of Information Technology, Modeling and Computing (IJITMC) 2 55-62.

[46] Sharma H, Sharma K K and Chauhan S 2014 Steganography Techniques Using Cryptography-A Review Paper.

[47] Dhamija A and Dhaka V 2015, October A novel cryptographic and steganographic approach for secure cloud data migration In Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on (pp. 346-351) IEEE.

[48] Vijayakumar P, Vijayalakshmi V and Zayaraz G 2016 An improved level of security for dna steganography using hyperelliptic curve cryptography Wireless Personal Communications 89 1221-1242.

[49] Patil S S and Goud S 2016 Enhanced Multi Level Secret Data Hiding In An International Conference.

[50] Karthikeyan B, Kosaraju A C and Gupta S 2016 March Enhanced security in steganography using encryption and quick response code In Wireless Communications, Signal Processing and Networking (WiSPNET), International Conference on (pp. 2308-2312) IEEE.

[51] Pillai B, Mounika M, Rao P J and Sriram P 2016 September Image steganography method using K-means clustering and encryption techniques In Advances in Computing, Communications and Informatics (ICACCI), 2016 International Conference on (pp. 1206-1211) IEEE.

[52] Hingmire A, Ojha S, Jain C, Thombare K 2016 Image steganography using adaptive b45 algorithm combined with pre-processing by twofish encryption International Educational Scientific Research Journal 2 4.

[53] Joseph F and Sivakumar A P S Advanced security enhancement of data before distribution.

[54] Padmavathi B and Kumari S R 2013 A survey on performance analysis of DES, AES and RSA algorithm along with LSB substitution IJSR, India.
[55] Das R and Tuithung T 2012 March A novel steganography method for image based on Huffman Encoding In Emerging Trends and Applications in Computer Science (NCETACS), 2012 3rd National Conference on (pp. 14-18) IEEE.

[56] Muhammad K, Ahmad J, Sajjad M and Zubair M 2015 Secure image steganography using cryptography and image transposition arXiv preprint arXiv:1510.04413.

[57] Barhoom T S and Mousa S M A 2015 A Steganography LSB technique for hiding Image within Image Using blowfish Encryption Algorithm Int. J. Res. Eng. Sci, 3 61-66.

[58] Thomas S E, Philip S T, Nazar S, Mathew A and Joseph N 2012, May Advanced cryptographic steganography using multimedia files In International Conference on Electrical Engineering and Computer Science (ICEECS-2012).

[59] Muslim M A and Prasetyo B 2015 Data hiding security using bit matching-based steganography and cryptography without change the Stego image quality Journal of Theoretical & Applied Information Technology 82 1.

[60] Gambhir A and Mishra A R 2015 A New Data Hiding Technique with Multilayer Security System.

[61] Sharma M H, MithleshArya M and Goyal M D 2013 Secure image hiding algorithm using cryptography and steganography IOSR Journal of Computer Engineering (IOSR-JCE).

[62] Sharma M H, MithleshArya M and Goyal M D 2013 Secure image hiding algorithm using cryptography and steganography IOSR Journal of Computer Engineering (IOSR-JCE).

[63] Mishra M, Tiwari G and Yadav A K 2014 May Secret communication using public key steganography In Recent Advances and Innovations in Engineering (ICRAIE), 2014 (pp. 1-5) IEEE.

[64] Kumar R H, Kumar P H, Sudeepa K B and Aithal G 2013 Enhanced security system using symmetric encryption and visual cryptography International Journal of Advances in Engineering & Technology 6 1211.

[65] Sridevi D R, Vijaya P and Rao K S 2013 Image steganography combined with cryptography Council for Innovative Research Peer Review Research Publishing System Journal: IJCT 9 1.

[66] Almuhammadi S and Al-Shaaby A 2017 A survey on recent approaches combining cryptography and steganography Computer Science Information Technology (CS IT).