A Survey On Combined Various Data Hiding Techniques

[1*]Ali Abdulraheem Alwan, [2]Mohd Shahidan Abdullah, [3]Nilam Nur Amir Sjarif

Razak Faculty of Technology & Informatics, University Technology Malaysia, 54100 Kuala Lumpur, Malaysia.

[1] aliraheem1983@gmail.com, [2] mshahidan@utm.my, [3] nilamnur@utm.my,

Article history

Received:
30 Sept 2019

Received in revised form:
20 Oct 2019

Accepted:
20 Dec 2019

Published online:
30 Dec 2019

*Corresponding author
aliraheem1983 @gmail.com

Abstract

The process of hiding an information in a carrier is referred to as data hiding and there are several methods for this process even though there are certain advantages and drawbacks of most of these methods.one or more data hiding methods can be deployed at the same time depending on the type and level of the intended application. Data information can be hidden in several forms of carriers such as audios, texts, video, protocol, image, and DAN. Some of the digital image data hiding methods pay more attention to image security while some focus on the robustness of the image hiding process and on the imperceptibility of the hidden image. One of the major concern in certain applications is the capacity of information to be hidden in the carrier; as such, the major aim of some previous studies has been to achieve two or more of hidden images' security, imperceptibility, robustness, and capacity. However, some of these image parameters are sometimes complimentary as only one can be realized at the expense of the other. In this paper, some of the existing digital image hiding techniques were reviewed while a comparative study was conducted between 3 of these hiding techniques.

Keywords: *Cryptography; steganography; watermarking.*

1. Introduction

Digital information is a common phenomenon in recent times due to the increase in the digitization of virtually every aspect of life. As such, the conventional data hiding methods have been upgraded and modified in recent times to ensure the integration, security, and confidentiality of digital information and to ensure their compatibility with other schemes. This has led to the development of various schemes for the protection and security of digital information and such methods include cryptographic, steganographic, watermarking methods, as well as their combinations. These schemes are faced with different challenges and have different aims to be achieved. These aims particularly depend on the considered application area in which digital information is either deployed or manipulated. Some of the problems associated with these schemes are the security, fragility, and robustness of the data

** Corresponding author. aliraheem1983@gmail.com*

hiding process. As a benchmark, some parameters are considered when determining the suitability of a scheme and the values of these parameters vary with the application domains. Information encryption, also called cryptography, is a process of scrambling a secret information to an extent that it will be difficult to eavesdrop. Cryptography, however, has been reported to be inefficient in completely encrypting a secret message and this has received attention in recent times [1, 2].

Hence, there is a need for a scheme which can guarantee an invisible communication (communicating without anyone noticing the existence of such communication) and this has given rise to the development of the steganographic and watermarking techniques [1].Both watermarking and steganographic techniques ensure the hiding of secret messages, and they are closely related although with different objectives. The steganographic methods mainly aim at concealing the presence of communication and secret data protection [3] while watermarking aims at protecting the integrity of secret data with or without hiding the presence of such information from eavesdroppers [4]. By combining the cryptographic, steganographic, and watermarking techniques or combining any two of these techniques, a better image security can be achieved by hiding the existence of encrypted messages [2]. This paper presents an overview and a comparative study of the basic information hiding techniques and the related works on digital data hiding techniques.

2. Data Hiding Techniques

These are the techniques used to hide data to keep it safe from third party capturing or modification. Some of the techniques for data hiding are depicted in Figure 1 [5].

Figure 1. Classification of data hiding techniques

2.1 Steganography

Steganography refers to the science of concealing the presence of secret information using digital communication objects [3]. As shown in Figure 2, the communication object can be any medium, service or device which is used for any form of secret communication [6]. The communication carriers are generally digital files such as images, texts, videos, audios, DNA, and network protocol.

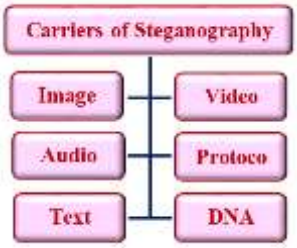


Figure 2. Digital carriers of steganography

Different digital media embeds secret information using different characteristics; for instance, text steganography achieves secret communication by utilizing line/word shifting encoding emoticons in textual chat [7]. Emoticons have recently been used in textual chat for secret communication [8]. During audio steganography, spread spectrum, phase coding, and low-bit encoding are mainly employed to embed secret information [9]. Secret data can as well be concealed into packet headers and payload packet in another medium such as network protocol [10], while retransmission steganography (i.e. packet acknowledgment and forwarding) can also be used during retransmission steganography [11]. For the DNA-based steganographic methods, secret data can also be embedded using the randomness features of DNA. The numerical mapping table has recently been used for DNA sequence mapping for encoding secret information [12]. In video steganography, a combination of audio and image steganography is often utilized. It has more capacity to embed more secret data due to the combination of different images in a video stream [13]. In image steganography, an image is used as the carrier to hide the secret information; a basic image steganographic scheme is depicted in Figure 3 in which the image is denoted by the term 'cover image' used to embed the secret data or 'secret message'. An embedding technique generally refers to the algorithm or the procedure used to embed the secret message in the cover image to generate the stego-image using an optional stego-key. The stego-key must be available to both the sender and receiver of the message as it will be used by the receiver to extract the hidden information from the carrier.

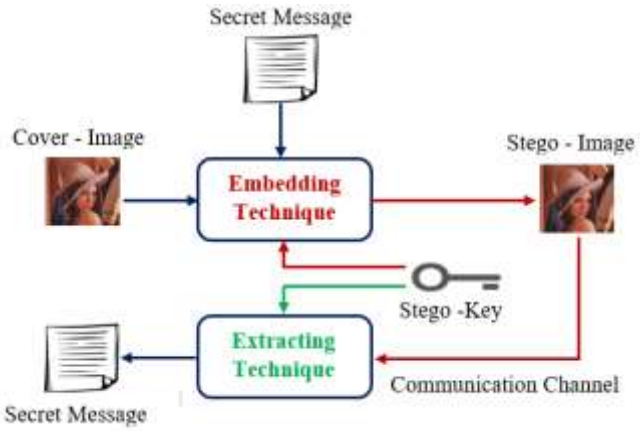


Figure 3. Block diagram of steganography process

However, an attack on a steganographic process is referred to as steganalysis which is defined as the act of detecting the presence of a secret message or its recovery from the stego-images. Meanwhile, there are two attributes of any secret message embedding medium first, it must be popular, and secondly, it must be able to conceal any modification in the cover medium [14]. Until now, the available digital steganography literature focused mainly on the use of image as the commonest medium for information hiding due to the following reasons [15-17]:

a. It is the most widely used medium.
b. Takes advantage of the limited visual perception of colors.
c. This field is continually growing with the growth of computer graphics.
d. Digital images are made up of pixels.
e. The arrangement of pixels makes up the image's '*raster data*'.
f. 8-bit and 24-bit images are common.
g. The larger the image size, the more information can be hidden.
h. Digital images often have a large amount of redundant data.

2.2 Cryptography

The word cryptography is made up of two words, "crypto" and "graphy" (derived from the Greek language) which means hidden writing. Cryptography is a process in which a dataset is transformed into a text form that is difficult to be interpreted by an unintended user. Such a text is also called the ciphertext [18]. The recipient of the encrypted text decodes or unscramble the message into the plaintext using a specific key. Cryptography ensures data secrecy, information uprightness, verification, and non-repudiation. Secrecy refers to restriction of access or putting a limitation on specific sorts of data while integrity refers to keeping up and guaranteeing the precision of information being conveyed (i.e. no data alteration or cancellation). Verification, on the other hand, guarantees the authenticity of the data sender and recipient. Non-denial is the capacity to guarantee that the sender or recipient of the message cannot prevent the realness from securing their mark on the sending data that they began [5].

The current age cryptography is synonymous with encryption [19]. Here, the first data is known as the plain content and the scrambled data is known as the ciphered content. The process of cryptography works in three phases or the so-called steps: In the first step, the original message generated by the source is encrypted into the non-readable form. Such an unreadable message is also called the ciphertext and the complete process is called encryption. In the next step, the unreadable message or the ciphertext is transferred from the source to the destination through some transmission media. In the last step, the recipient of the message receives the ciphertext and decode it into the plaintext to get the original message [20]. The complete process of encryption and decryption is shown in Figure 4. This process of encryption can be performed in more than one way depending on the type of key used. One of the ways is called symmetric key cryptography and the other is called asymmetric key cryptography [5].

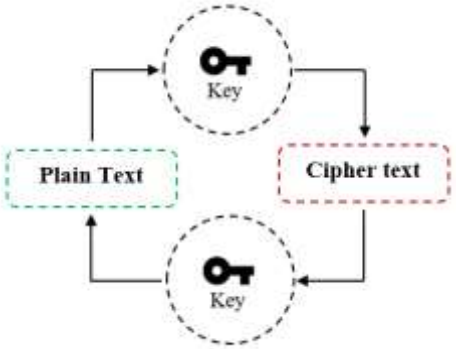


Figure 4. Block diagram of cryptography process

Symmetric key cryptography: This refers to the cryptographic strategies in which the sender and the receiver share a similar key [21]. Many encryption algorithms like AES, DES, and RC5 uses this methodology. Symmetric key cryptography consists of five major components, which are the original message (plain content), an algorithm for encryption, cipher content, key, and algorithm for decryption. An algorithm for encryption is used for performing several operations on the plaintext using the secret key. The secret key used is independent of the plaintext and is chosen by either the sender or the receiver of the message. The receiver uses the decryption algorithm to transform the ciphertext back into the plaintext with the help of the secret key known only by the sender and the receiver. The process of symmetric key cryptography is shown in Figure 5. A noteworthy limitation of symmetric key encryption is that it requires the key to be shared by each of the conveying parties, and furthermore, the key itself must be transmitted through a secured medium as any unintended access to the key is a threat to the whole process.

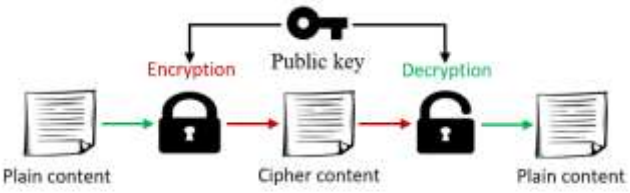


Figure 5. Symmetric key cryptography diagram

Asymmetric key cryptography: In this type of encryption technique, two types of keys are used; one of the keys is called the private key and the other one is called the public key. The sender transforms the original message into the ciphertext using a public key. Then, the ciphertext is transmitted to the intended user through some transmission media; finally, the receiver uses the private key to decrypt the message to get the original message [22]. The process of asymmetric key cryptography is shown in Figure 6.

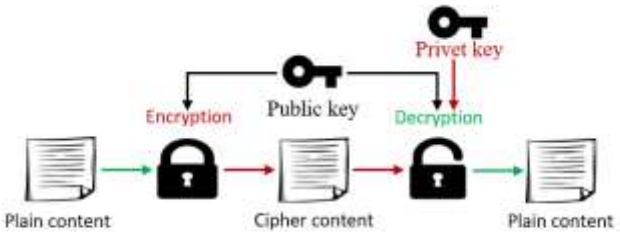
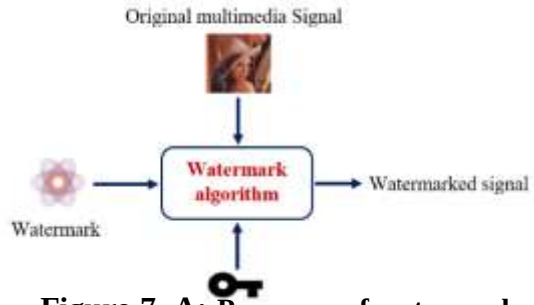


Figure 6. Asymmetric key cryptography diagram

2.3 Watermarking

The art of digital watermarking dated back to 1979 but did not receive enough attention until 1990 and full application around 1998. Although its invention cannot be credited to a person, yet, it is still gaining interest today, and unlike Napster, it is proving to be an indispensable process [23]. The act of digital watermarking refers to the embedding of a signature signal (known as a watermark) into a digital cover for several reasons such as ownership verification, authenticity check, cover image integrity check, and may be applied to both text, audio, video, and images [24]. During a watermarking process, a watermark or digital signature is embedded into a digital object such that the embedded watermark can be extracted later to make an assertion about the object. However, additional information such as the identity of the buyer of a certain copy of a material may be contained in the watermark. The processes of watermark embedding, and extraction are depicted in Figures 7(a) and (b), respectively [25]. As earlier mentioned, digital watermarking is closely related to steganography; therefore, digital watermarking refers to the process of concealing a secret message to ensure its copyright and integrity protection. A watermark may also confer several security features to the document, such as serial numbers and other data related information. A watermarked data can provide information on the upgrading or modifications of a data, as well as counterfeits through a comparison of the watermarked data to the original data [26]. The actual content of a watermark is dependent on the requirements for information integrity protection, as well as on the documents' authentication. There are two classes of digital watermarking which as private and public watermarks [26].



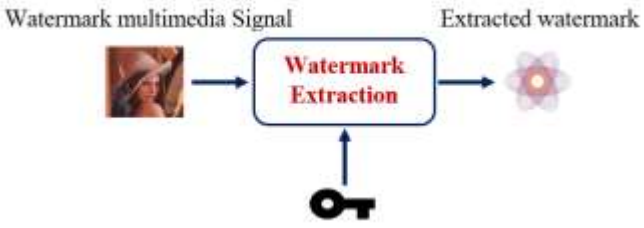


Figure 7. A: Processes of watermark embedding. Figure 7.B Processes of watermark extracting.

A. Private watermark

A private (secret) watermark provides additional information for the identification of a licensee or for ownership proves during disputes. At least one secret key which is known to the embedder alone is required to retrieve information from a private watermark. A private watermarking process requires a robust watermarking algorithm although the performance requirements may be relaxed. In a private watermark, information such as the licensee-identification hash values, or serial numbers is embedded. A serial number is generally a link to an externally stored information, such as a customers' record [27].

B. Public watermark

Here, a public watermark is extracted by the licensee of the copyrighted material. Usually, a public watermark contains a licensing or copyright information such as a patent identifier, a copyright holder, a link to additional information, or a creator of the material. A public watermark demands a watermarking algorithm with enough capacity. Being that it provides additional information related to copyright for the receivers and does not aim at ownership proves, it does not demand much algorithmic robustness [28]. Generally, there are 3 parts of any watermarking algorithm, including the watermark itself, the watermark insertion algorithm or the encoder, and the decoder and comparator [29]. Each owner has a unique watermark and each owner can embed different watermarks in different objects using the marking algorithm. The object is authenticated by the verification algorithm to determine both the objects' owner and its integrity as well.

3. Related Work

A framework for the decomposition of medical images into the region of interest (ROI) and region of non-interest (RONI) has been proposed by [32]. Here, 3-level DWT is applied on the RONI part while 3 watermarks (authentication, integrity, and tamper localization watermarks) but later 2 are generated as a hash value and CRC-16 value from the ROI part. This method first decomposes the image into 4 sub-bands (LL1, HL1, LH1, and HH1) by applying a DWT on the RONI part before applying a 2-DWT on the HL1 sub-band to decompose it further into 4 sub-bands bands (LL2, HL2, LH2, and HH2). Next, the HL2 sub-band is further decomposed into 4 sub-bands (LL3, HL3, LH3, and HH3) by applying a 3-DWT is applied on the HL3 sub-band. The patients' information is then embedded in the HL3 sub-band as a watermark before applying an inverse DWT. After applying the inverse DWT, the integrity watermark is embedded into the HL2 sub-band, followed by another inverse DWT. At last, the tamper localization watermark is embedded into the HL1 sub-band followed by an inverse DWT. Finally, the ROI and RONI are combined to get the original watermarked image. This method guarantees a high security and imperceptibility.

A method for digital image authentication and copyright protection where the cover image (CI) is first partitioned into 64 blocks, followed by a calculation of the entropy of each block, has been proposed by [33]. The watermarked image is resized to the block size of the CI and hidden in the blocks with the highest entropy using an LSB embedding

method. This method produces good MSE and PSNR values which confirms the robustness and perceptibility of the watermarked image, but there is no report on its performance against attacks.

A watermarking method which deploys arithmetic progression to give a higher robustness and perceptibility against various attacks has been proposed by [34]. This method first converts a cover RGB image into a grayscale image of 512 x 512 size before applying a 2-DWT on the converted image to generate 4 sub-bands (LL1, HL1, LH1, and HH1) of 256 x 256 size. Next, a QR-code image is produced and converted into the grayscale image before being converted into a binary image of 48 x 48 size. It is then, taken as the watermarked image and resized to 1 x 2304 size before being further resized into 3 x 768. The average of each sub-band (i.e. HL1, LH1, and HH1) is then, calculated and the least average sub-band is embedded first before embedding the others with a higher average. The 1 x 768 components of the watermark are taken and resized into 256 x 3 components. Then, an equation is used to identify the positions to insert the watermark in the sub-bands before using an arithmetic progression technique to insert the watermark. Finally, the final watermarked image is achieved by performing an inverse 2-DWT. This scheme is comparatively robust against several attacks as indicated by its PSNR value which is consistently more than 50 db.

A robust blind watermarking framework based on both Redundant Second-Generation Wavelet Packet Transform (RSGWPT) and Modified Fast Haar Wavelet Transform (MFHWT) has been proposed y [35]. Here, the original cover image is decomposed with the MFHWT until its sub-images size is 4 times the size of the watermark image before applying the RSGWPT to the last decomposition of MFHWT. For an improved security, the security pixels of the watermark is distributed on all the sub-images. Then, each pixels' grayscale value is calculated and partitioned into 3 parts (A, B, and C) which are further decomposed into 4 bands of equal size with the watermark. Then, A, B, and C are embedded into the remaining bands except the first one. To ensure the invisibility of the process, the watermark is embedded into the fine-scaled frequency bands of the RSGWPT with the least match after the coefficients of RSGWPT have been compared with A, B, and C. Finally, the original watermarked image is obtained by performing the inverse of MFHWT and RSGWPT. The scheme is reported to be robust against several attacks such as Poisson and Speckle noise and Salt and Pepper attacks. Its watermark embedding and extraction processes are faster and it provides better PSNR and NC values although its application is a bit complicated.

A dual-purpose robust spatial domain cryptographic and digital watermarking algorithm in which key is generated using an Extended Hamming code has been proposed by [36]. An Extended Hamming Code is used to extract and process the cover images' LSB before embedding the messages pixels (in case of watermarking); and for the encryption aspect, the key pixels are converted into 8-bit binary value before extracting the LSB of the second-bit plane and XORing with the message pixel value. The Extended Hamming code is used to code the outcome of this process and the LSB of the second-bit plane into 4-bit codes. This method presents a high level of robustness and imperceptibility, but it depends on the spatial domain instead of the frequency domain.

A method for the provision of a high level of security based on the use of a combined steganographic, cryptographic, and watermarking features has been proposed by [37]. This method divides a binary image into 8 x 8 blocks before applying a zigzag hiding sequence on each block to conceal the path of the hidden data. The data encrypted image is then created using a (2, 2) VC share technique where it is impossible for someone with only one share to reveal the secret information. Then, an LSB method is deployed to embed the generated shares into separate cover images to achieve digital watermarking. This method provides a good visual quality and an advanced level of security using steganography, but it requires more processing time owing to the complexity of the steganographic algorithm.

A system for the embedding of large information in an image with no significant alteration of the information quality during the processing has been proposed by [38]. The original image (OI) and the watermark image (WM) are resized in the proposed scheme to N*N with a subsequent separation of their RGB components. Then, both images are divided into low and high-frequency components by applying a 2-level DWT. To embed the separated OI components, the WM components are multiplied by a scaling factor to generate a new image. After generating the new image, an inverse 2DWT is further applied to the 2-DWT transformed image to produce the original WM image. To detect any alteration, the OI and WM are used as reference images. In addition to embedding large sized information and limiting the observable alteration, this method provides a good PSNR value although it losses significant information at a high level of DWT. The robustness of the system against cropping and rotation attacks are not reported.

A scheme that uses medical images as a carrier for embedding patients' information as a binary WM image without having any significant effect on the image quality has been suggested by [39]. In this system, a DWT is first applied on host image for the generation of 4 non-overlapping multiresolution coefficient sets (LL, HL, LH, and HH) before dividing the LL sub-band into 3 x 3 non-overlapping blocks. Then, a calculation of the gray differences between the center and the neighboring pixels is performed, taking the center pixel value as the threshold and assigning them with binary bits (1 and 0). An XOR operation is performed on the obtained binary bits to produce the Logistic map while a chaotic watermark is generated by XORing the generated logistic map and the binary watermark image. The generated chaotic watermark bits are then embedded into the host images' LL sub-band with respect to the conditions of the neighboring pixels. Finally, the original watermarked image is obtained by performing an inverse DWT. This method achieved a good PSNR and NC value and maintained a good watermarked image and extracted watermark quality.

An algorithm for the generation of two shares based on VCS has been proposed by [40]. One of the shares is embedded into the DCT coefficients of color images' blue components while the other is copyright protected. In this method, two shares (S1 and S2) are generated using an XOR-based (2, 2) VCS algorithm. First, the blue component of a color image is decomposed into non-overlapping 8 x 8 blocks before applying DCT on each block. Then, the S1 is now embedded into these blocks while an inverse DCT is applied to obtain the original watermarked image color. The S2 is copyright protected and is used for the recovery of the watermark. The method achieved a good NC value but its PSNR value is not up to the acceptable level compared to the other schemes.

An encryption technique which uses Elliptic Curve Cryptography (ECC) during and before JPEG compression has been suggested by [41]. The ECC is a suitable method in environments with power, storage, and bandwidth constraints. The ECC is jointly applied to the proposed method with an independent compression scheme. To ensure a perceptual encryption, the ECC is applied after transforming the encoded and quantized image to achieve a selective encryption and decryption process prior to the compression process. The proposed method uses 2 ECC-based algorithms which is a selective encryption of the quantized DCT coefficients and a perceptual encryption based on selective bit-plane encryption. The good aspect of this scheme is its fastness and security; similarly, it has no effect on the compressed data, but the applied codec is needed for the modification if ECC is applied during the compression process.

A biometric system which is based on vector quantization watermarking and on LBG algorithm has been proposed by [42]. Here, the LBG or the generalized Lloyd algorithm (GLA) are used to embed iris information of eye image in the fingerprint image to ensure their security. This method used two databases for the fingerprint and iris images. An XOR operation is first performed in this method on the 2 binary Iris images to generate the permutated version of the watermark; then, the fingerprint image is further decomposed into 2 x 2 blocks to achieve the quantified vectors. The LBG algorithm and the current dictionary are then used to get the quantized fingerprint image X'. The differences in the indices of the quantization vectors are calculated based on some threshold values to obtain the binary polarity matrix P. Finally, an XOR operation is conducted on P using the permutated watermark to achieve the Key that will be transmitted to the recipient along with X. This system provides a good level of security and robust against several attacks. A summary of the reviewed methods in this study is presented in Table 2.

Table 2: **A review on various data hiding technique**

Ref No.	Authors and year	Objectives	Techniques	PSNR (db) Up to
[32]	Al-Haj, Hussein, & Abandah (2016)	To ensure a secure medical image transmission using a hybrid encryption and watermarking technique.	3 level DWT and 3 different Watermarks	98.1093
[33]	Kumar & Dutta (2016)	Copyright protection and authentication of the image.	Block entropy and spatial domain LSB insertion watermarking technique	69.2377
[34]	Malonia & Agarwal (2016)	Development of a watermarking techniqu with an enhanced imag perceptibility and improved robustness against several attacks.	DWT, watermarking using Arithmetic progression	79.8547
[35]	Kaur & Lal (2015)	Provision of a high quality watermarked	MFHWT decomposition and RSGWP	55.18

		image with the aid of a modified Fast Haar WT and Redundant Second Generation WPT through blind watermarking.		
[36]	Ghosh, De, Maity, & Rahaman (2015)	Development of a blinc watermarking scheme in spatial domain with self-correcting capability for both cryptographic and watermarking applications.	Extended Hamming code and Watermarking	81.78
[37]	Gayathri & Nagarajan (2015)	Provision of an enhanced level of security by deploying a combined steganographic, cryptographic, and watermarking features.	Visual Cryptography, Steganography and Invisible Watermarking using LSB insertion technique	55.9110
[38]	Rajawat & Tomar (2015)	Image security enhancement by using two-level DWT on the RGB components of th OI and image watermarking through combined tamper detection and watermarking method.	Separation of RGB component, 2 level DWT and watermarking	61.62
[39]	Moniruzzaman, Hawlader, & Hossain (2014)	The use of DWT and chaotic techniques for the authentication of patient's information. the method also aims to preserve image quality.	DWT and Chaotic Watermarking using Logistic map	49.58
[40]	Han, He, Ji, & Luo (2014)	To enhance the embedding capacity and robustness of watermarks.	DCT, Visual Cryptography and Watermarking	42.008
[41]	Bakhtiari, Ibrahim, Salleh, & Bakhtiari (2014)	Use of ECC to secure JPEG images during and before image compression.	Two ECC based encryption algorithm: selective encryption of the quantized DCT coefficients for during compression and perceptual encryption based on selective bitplane encryption	17.70

[42]	Ouslim, Sabri, & Mouhadjer, (2013)	Enhancement of the robustness and security of digital images through a combination of two biometric signatures using watermarking and cryptographic methods	Vector Quantization Watermarking based on LBG algorithm and Chaotic Cryptography	10

4. Conclusion

Data hiding is a good solution for the confidentiality and integrity of data from third-party attacks. By merging steganographic, watermarking, and cryptographic techniques or by merging two of the three can provide more security for data confidentiality. For example, steganography and cryptography can provide two levels of security for the transmitted information as the intruders cannot easily damage the system even if they are aware of the secret data since they cannot easily recognize the data because it is hidden in two stenographic and cryptographic methods which will certainly take time to open with different algorithms. The major focus in this paper is on the related works on various data hiding techniques as well as their comparison. Each technique has its own merits and challenges and is applicable to different application domains. Some of the reviewed studies mainly aim at achieving like two or more from these requirements as to the security, robustness, imperceptibility, and capacity. However, some of these parameters cannot be achieved together as the only one can be achieved at the expense of the other. Hence, data hiding techniques that aim at achieving maximum requirements can be deployed in the larger application domains when desired.

Acknowledgments

The authors would like to thank Universiti Teknologi Malaysia (UTM) for their educational and financial support. This work is conducted at Razak Faculty of Technology & Informatics.

5. Reference

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

[2] Singh, S., Singh, A. K., & Ghrera, S. P. (2017, February). A recent survey on data hiding techniques. In *I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2017 International Conference on* (pp. 882-886). IEEE.

[3] Maurya, I., & K Gupta, S. (2018). Understandable Steganography. *International Journal of Engineering & Technology*, *7*(3), 1024-1033. doi:http://dx.doi.org/10.14419/ijet.v7i3.8940

[4] Nagaraju, G., Pardhasaradhi, P., & S. Ghali, V. (2018). A New Watermarking Scheme for Medical Images with Patient's Details. *International Journal of Engineering & Technology*, *7*(3.31), 25-29. doi:http://dx.doi.org/10.14419/ijet.v7i3.31.18194

[5] Gupta, A., Verma, P., & Sambyal, R. S. (2018). A Comparison of Different Data Hiding Techniques.

[6] Mazurczyk, W., & Caviglione, L. (2015). Steganography in modern smartphones and mitigation techniques. *IEEE Communications Surveys & Tutorials*, *17*(1), 334-357.

[7] SHAKIR BAAWI, S. A. L. W. A., ROSMADI MOKHTAR, M. O. H. D., & Sulaiman, R. (2017). NEW TEXT STEGANOGRAPHY TECHNIQUE BASED ON A SET OF TWO-LETTER WORDS. *Journal of Theoretical & Applied Information Technology*, *95*(22).

[8] Liu, Y., Yang, T., & Xin, G. (2015). Text Steganography in Chat Based on Emoticons and Interjections. *Journal of Computational and Theoretical Nanoscience*, *12*(9), 2091-2094.

[9] Mudusu, R., Nagesh, A., & Sadanandam, M. (2018). Enhancing Data Security Using Audio-Video Steganography. *International Journal of Engineering & Technology*, *7*(2.20), 276-279. doi:http://dx.doi.org/10.14419/ijet.v7i2.20.14777

[10] Bagchi, R. (2017). Packet Payload for Network Steganography.

[11] Mazurczyk, W., Smolarczyk, M., & Szczypiorski, K. (2011). Retransmission steganography and its detection. *Soft Computing*, *15*(3), 505-515.

[12] Malathi, P., Manoaj, M., Manoj, R., Raghavan, V., & Vinodhini, R. E. (2017). Highly Improved DNA Based Steganography. *Procedia Computer Science*, *115*, 651-659.

[13] Mudusu, R., Nagesh, A., & Sadanandam, M. (2018). Enhancing Data Security Using Audio-Video Steganography. *International Journal of Engineering & Technology*, *7*(2.20), 276-279. doi:http://dx.doi.org/10.14419/ijet.v7i2.20.14777

[14] Zielińska, E., Mazurczyk, W., & Szczypiorski, K. (2014). Trends in steganography. *Communications of the ACM*, *57*(3), 86-95.

[15] Chavan, N. S. (2015). IMAGE STEGANOGRAPHY–AN OVERVIEW. *International Journal of Recent Scientific Research*, *6*, 4800-4804.

[16] Kumari, T., & Singh, K. (2018). A Review on Information Hiding Methods. *International Journal of Engineering Science*, *17474*.

[17]Laishram, D., & Tuithung, T. (2018). A Survey on Digital Image Steganography: Current Trends and Challenges.

[18] Gupta, A., & Walia, N. K. (2014). Cryptography algorithms: A review.

[19] Gupta, R., Gupta, S., & Singhal, A. (2014). Importance and techniques of information hiding: a review. *arXiv preprint arXiv:1404.3063*.

[20] Boneh, D., & Franklin, M. (2001, August). Identity-based encryption from the Weil pairing. In *Annual international cryptology conference* (pp. 213-229). Springer, Berlin, Heidelberg.

[21] Delfs, H., & Knebl, H. (2015). Symmetric-Key Cryptography. In *Introduction to Cryptography* (pp. 11-48). Springer, Berlin, Heidelberg.

[22] Chaudhury, P., Dhang, S., Roy, M., Deb, S., Saha, J., Mallik, A., ... & Das, R. (2017, August). ACAFP: Asymmetric key based cryptographic algorithm using four prime numbers to secure message communication. A review on RSA algorithm. In *Industrial Automation and Electromechanical Engineering Conference (IEMECON), 2017 8th Annual* (pp. 332-337). IEEE.

[23] Pal, M. (2016). A survey on digital watermarking and its application. *International Journal of Advanced Computer Science and Applications*, *7*(1), 153-156.

[24] Guru, J., & Damecha, H. (2014). Digital watermarking classification: a survey. *International Journal of Computer Science Trends and Technology (IJCST) vol*, *5*, 8-13.

[25] Mohanty, S. P. (1999). Digital watermarking: A tutorial review. *URL: http://www. csee. usf. edu/~ smohanty/research/Reports/WMSurvey1999Mohanty. pdf*.

[26] Jain, J., & Rai, V. (2012). Robust Multiple Image Watermarking Based on Spread Transform. In *Watermarking-Volume 2*. InTech.

[27] Tonge, M., Malviya, P. K., & Gupta, A. (2014). Implementation of Digital Watermarking Algorithm based on DWT and DCT. *International Journal of Advanced Engineering and Global Technology*, *2*(1).

[28] Jiang, F. (2017). *Efficient Public-Key Watermark Techniques for Authentication* (Doctoral dissertation, Purdue University).

[29] Singh, P., & Chadha, R. S. (2013). A survey of digital watermarking techniques, applications and attacks. *International Journal of Engineering and Innovative Technology (IJEIT)*, *2*(9), 165-175.

[30] Desai, H. V. (2013). Steganography, Cryptography, Watermarking: A Comparitive Study. *Journal of Global Research in Computer Science*, *3*(12), 33-35.

[31] Koppu, S., & Viswanatham, V. M. (2017). A fast enhanced secure image chaotic cryptosystem based on hybrid chaotic magic transform. *Modelling and Simulation in Engineering*, *2017*.

[32] Al-Haj, A., Hussein, N., & Abandah, G. (2016, May). Combining cryptography and digital watermarking for secured transmission of medical images. In *Information Management (ICIM), 2016 2nd International Conference on* (pp. 40-46). IEEE.

[33] Kumar, S., & Dutta, A. (2016, April). A novel spatial domain technique for digital image watermarking using block entropy. In *Recent Trends in Information Technology (ICRTIT), 2016 International Conference on* (pp. 1-4). IEEE.

[34] Malonia, M., & Agarwal, S. K. (2016, March). Digital image watermarking using discrete wavelet transform and arithmetic progression technique. In *Electrical, Electronics and Computer Science (SCEECS), 2016 IEEE Students' Conference on* (pp. 1-6). IEEE.

[35] Kaur, S., & Lal, M. (2015, December). An invisible watermarking scheme based on Modified Fast Haar Wavelet Transform and RSGWPT. In *Recent Advances in Engineering & Computational Sciences (RAECS), 2015 2nd International Conference on* (pp. 1-5). IEEE.

[36] Ghosh, S., De, S., Maity, S. P., & Rahaman, H. (2015, December). A novel dual purpose spatial domain algorithm for digital image watermarking and cryptography using Extended Hamming Code. In *Electrical Information and Communication Technology (EICT), 2015 2nd International Conference on* (pp. 167-172). IEEE.

[37] Gayathri, R., & Nagarajan, V. (2015, April). Secure data hiding using Steganographic technique with Visual Cryptography and Watermarking Scheme. In *Communications and Signal Processing (ICCSP), 2015 International Conference on* (pp. 0118-0123). IEEE.

[38] Ghosh, S., De, S., Maity, S. P., & Rahaman, H. (2015, December). A novel dual purpose spatial domain algorithm for digital image watermarking and cryptography using Extended Hamming Code. In *Electrical Information and Communication Technology (EICT), 2015 2nd International Conference on* (pp. 167-172). IEEE.

[39] Moniruzzaman, M., Hawlader, M. A. K., & Hossain, M. F. (2014, December). Wavelet based watermarking approach of hiding patient information in medical image for medical image authentication. In *Computer and Information Technology (ICCIT), 2014 17th International Conference on* (pp. 374-378). IEEE.

[40] Han, Y., He, W., Ji, S., & Luo, Q. (2014, November). A digital watermarking algorithm of color image based on visual cryptography and discrete cosine transform. In *P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2014 Ninth International Conference on* (pp. 525-530). IEEE.

[41] Bakhtiari, S., Ibrahim, S., Salleh, M., & Bakhtiari, M. (2014, August). JPEG mage encryption with Elliptic Curve Cryptography. In *Biometrics and Security Technologies (ISBAST), 2014 International Symposium on* (pp. 144-149). IEEE.

[42] Ouslim, M., Sabri, A., & Mouhadjer, H. (2013, September). Securing biometric data by combining watermarking and cryptography. In *Advances in Biomedical Engineering (ICABME), 2013 2nd International Conference on* (pp. 179-182). IEEE.