International Journal for Modern Trends in Science and Technology, 8(12): 15-23, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0812004
Available online at: http://www.ijmtst.com/vol8issue12.html

A Review Based on Various Image Steganography Techniques used for secure communication

Umaria khanam[1*] | Sayiema Amin[2]

[1]Department of ECE, SSM College of Engineering (affiliated to the university of Kashmir, Srinagar), India
[2]Faculty of ECE Department, SSM College of Engineering (affiliated to the university of Kashmir, Srinagar), India

To Cite this Article
Umaria khanam and Sayiema Amin. A Review Based on Various Image Steganography Techniques used for secure communication. International Journal for Modern Trends in Science and Technology 2022, 8(12), pp. 15-23. https://doi.org/10.46501/IJMTST0812004

Article Info
Received: 16 November 2022; Accepted: 27 November 2022; Published: 03 December 2022.

ABSTRACT

With the increasing usage of the Internet, the security and privacy of data transmission are becoming a major concern. Many researchers in this field have exploited various data protection techniques to provide secure communications. This study examines several data protection techniques such as cryptography, watermarking, and steganography, and provides an overview of different techniques for data hiding in images (image Steganography Techniques). These techniques prevent unauthorized users from accessing confidential data. Finally, certain conclusions are drawn based on the results of the conducted survey.

KEYWORDS: secure communication; data hiding; steganography; cryptography; watermarking.

1. INTRODUCTION

In recent decades, the speed of multimedia data transmission over the internet has increased rapidly due to the advent of new communication technologies. Currently, people spend much more time on the internet with information becoming increasingly accessible and distributed through the internet. There's also a trend of using the internet for digital secret data transmission to replace the need to transmit physical files such as confidential information, medical information, or the data used by the military or by commercial businesses.

Nowadays, people are spending more time on the internet as information becomes more and more accessible and widely disseminated through the internet. However, while easy access to the internet is an attractive aspect, its public nature has become one of the biggest limitations due to malevolent attacks. In mitigating malicious attacks, information security plays an important role. For information security, several data protection methods, such as encryption, steganography, and watermarking techniques have been proposed. These techniques have their own advantages and disadvantages. Characteristics such as embedding capacity (EC) or payload, robustness, security, embedding rate (ER), signal-to-noise ratio (PSNR), the structural similarity index (SSIM) cost, computational complexity, and reliability define the efficiency of these methods. In cryptography, plaintext data are converted into an indecipherable form called encrypted data or cipher text.The drawback of cryptography is that third parties arealways aware of unintelligible data transmissions [1] . Data hiding involves hiding the data in a cover file before sending it to the network. The

primary benefit of data- hiding techniques over encryption is concealing the existence of secret information [2] . It helps in the resolution of communication secrecy issues by concealing confidential information from malevolent users. To provide multilayer security, and to increase the efficiency of communications, some applications simultaneously employ data hiding and encryption in the same process as In 2021 H. Abdulkudhur Mohammed et al. [1] encrypted the text with a Goppa code using the McEliece algorithm and embedded the ciphertext as a steganographic image with the LSB method. O. F. Abdelwahab et al. in 2021 [3] proposed a combination of RSA cryptography and LSB steganography to hide data with significant security and ideal invisibility and used the Huffman, RLE, or DWT method for data compression. This method has Av. PSNR of 34.96 dB & bit rate of 1.33 bpp for RLE encoding and Av. PSNR of 37.18 dB & bit rate of 0.92 bpp for Huffman encoding and Av. PSNR of 43.45 dB & bit rate of 1.58 bpp for DWT encoding. A. Gambhir et al. [4] proposed "an RSA cryptographic algorithm with image steganography and audio steganography" and "DES cryptographic algorithm with image steganography and audio steganography." The outcomes demonstrate that these techniques outperform the individual techniques. When transferring highly sensitive data, these methods can be used. Data hiding fulfills the role of confidential communication when it meets two important criteria. First, the stego/marked image quality should be similar to that of the original image quality (i.e; the cover image should have good values of PSNR and SSIM), to prevent adversaries from detecting it while it is being transferred. Second, it must be capable of securely transmitting a significant amount of confidential data to the receiver [5] . Over the years, researchers have offered various data- hiding techniques. In this study, we will discuss several methods for hiding data in digital images.

2. TECHNIQUES USED FOR SECURE COMMUNICATION:

Techniques such as encryption or cryptography, watermarking, and steganography, are some approaches that ensure the safety of transmitted data

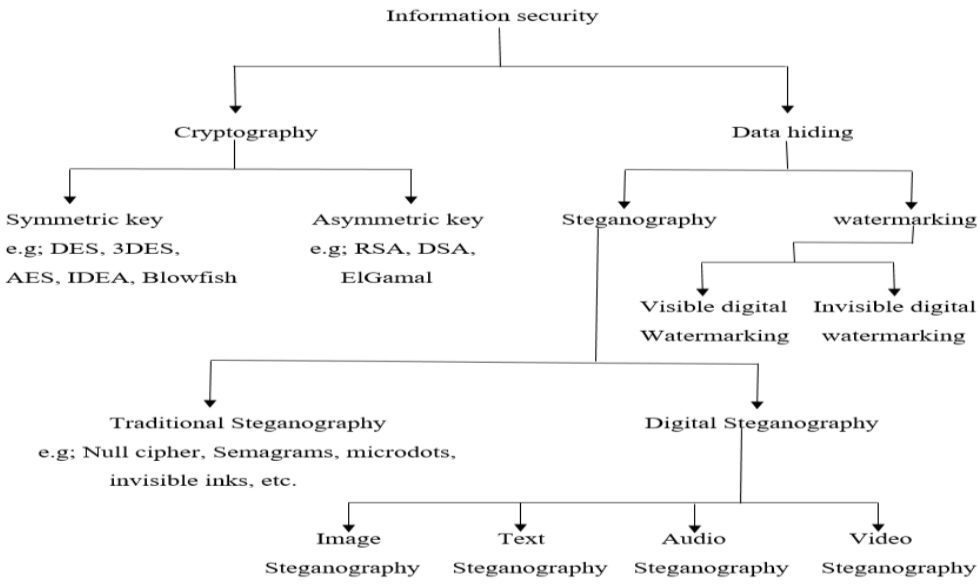

Figure 1: Information security techniques.

2.1 Cryptography:

The term cryptography comes from the Greek terms KRYPTOS, which means 'hidden,' and GRAPHEIN, which means 'writing or drawing,' that signifies 'secret or hidden writing.'[6] Cryptography is an intuitive way to protect confidential data. Here, confidential data are encrypted with an unreadable set of codes (cipher text) using encryption techniques, like data encryption standard (DES), 3DES, advanced encryption standard (AES), Rivest, Shamir, Adleman (RSA), Digital Signature Algorithm(DSA),Elgamal Algorithms, the international data encryption algorithm (IDEA), blowfish, McEliece cryptosystem, etc.[3][7][8][4]. With this method, only legitimate recipients with the Key can

access and decode the confidential data, whereas, illegitimate recipients in the absence of the Key are unable to discover the hidden data[7]. Still, Bob could not be prevented from observing the information, although it is unreadable and still exists as data, which could lead an invader to suspect covert communication[1]. In an attempt to solve this problem, an alternative method known as Steganography has been presented as a method for protecting sensitive data without drawing the attention of invaders. In recent times, some researchers have looked into cryptography techniques. In 2015, the performance of the widely used cryptographic methods DES, 3DES, AES, RSA, and blowfish was implemented and examined byP. Patil et al. The experimental findings clearly show that (1) blowfish requires the least amount of memory to implement, whereas RSA requires the most. DES and AES use medium-sized amounts of RAM.(2) compared to other algorithms RSA takes the maximum time for encryption and decryption, and Blowfish requires the minimum. (3) Blowfish performs well on software platforms. (4) Applications where
maintaining confidentiality and integrity is of the utmost importance can use the AES algorithm.(5)The blowfish is best at guessing attacks.(6)DES is the ideal method to use if the network capacity is a significant consideration in the application [7]. In 2021 R. Abid et al.presented a merge of the RSA method with the homomorphic encryption Chinese remainder theorem (HE-CRT) algorithm to provide quick communications. The HE-CRT-RSA uses multiple keys to facilitate efficient and secure communication. It is perceived that HE-CRT-RSA is 3 to 4% faster than traditional RSA [8].

2.2 Steganography:

The term steganography is derived from the Greek terms STEGANOS, which means "concealed or covered," and GRAPHEIN, which means "writing or drawing," i.e; concealed writing[6]. It is the technique of hiding or embedding the image, video, or message, in some other message, image,audio, or video, i.e; the cover medium or host data, without causing any suspicion of an attacker. Data hidden in the cover medium can be searched and discovered by the legal recipient only[9][10].In steganography, unlike cryptography, there is no need to send a separate key. Cryptography encrypts or scrambles a message and makes it incomprehensible, but Steganography serves the objective of hiding the message's existence[3]. Steganography comprises a wide variety of techniques for concealing the existence of secret information. Traditional methods include the use of null cipher, Semagrams, microdots, invisible inks, etc[2]. In modern times, steganography techniques use digital media like audio files, images, and video files.In 2015, D. Baby et al. proposedasteganography method to hide numerous color images into a single color image using the discrete wavelet transform. The R,G, and B components of the cover image are separated and theseplanesareembeddedwithsecretimages.The cover image and hidden image are broken down on an N-levels, and some of their frequency components are integrated. The stego image is then used to extract hidden images.

The results show that this approach has an average PSNR of 55.53 [9]. In 2016 G. Swain et al.presented a steganographic method based on 3D PVD and LSB substitution in 2*2 blocks of an image.Every 2x2 pixel block has K-bits of data inserted in the upper-left pixel using LSB substitution.Thatpixel'snewvalueisthenusedtocalculateth etopleft,bottomleft,andbottomrightpixeldifferences.Thed atabitsarethenconcealedusingthesethreedifferent values.This technique has two different variations; version 1 attains a PSNR of 40.44 and an embedding capacity of 2368750, and version 2 attains a PSNR of 39.29 and an embedding capacity of 2496419[10].

2.3 Watermarking:

Another important area of data hiding is copyright marking. It uses the inserted message to claim the copyright of the document. This can be done by the watermarking technique. As the steganography method is used for protection against detection, watermarking techniques are used for protection against removal. The digital watermarking technique is used to authenticate the cover message[11][12]. Similar to steganography, this is the procedure for embedding little signals (such as image caption, author signature, and authentication code) called a ‘watermark’ into digital content (like image, audio, text, video, etc.) these watermarks could later be disclosed or retrieved through computational operations to assert claims on the digital products[6]. The watermark is hidden inside the host data in such a way

that it cannot be separated from it, thus resisting any hostile actions. Watermarking is a viable option for protecting copyright, content validation, tamper detection, and more[13]. Unlike steganography, where covert data is unrelated to cover data and the cover image is viewed as a ruse to hide the presence of communication, this method links hidden data to cover data[2].M. Li et al. in 2020 consider using the Quaternion Discrete Fourier Transform (QDFT) and Quaternion QR (QQR) decomposition to watermark color images.The entropy value of each block is calculated for the scalar portion of the quaternion matrix created by the QQR decomposition, which was initially used in digital watermarking technology. The watermark is embedded and extracted from the block with the highest entropy. The outcomes demonstrate that this approach successfully strikes a balance between imperceptibility and resilience [11].In 2019 Q. Su et al.introduced a spatial domain watermarking method for color images to safeguard their copyrights. First, the DC coefficients of 2D-DFT are determined in the spatial domain,andthentheDCcoefficientdistributionruleisdeduced.This watermarking technique is a blind watermarking technique.The results of the experiments demonstrate that this method satisfies the requirements of invisibility and performs better in terms of robustness and real-time characteristics[12].

3. DATA HIDING IN IMAGES (IMAGE STEGANOGRAPHY) BASED ON AN EMBEDDING MECHANISM:

The two primary categories of data-hiding strategies are reversible and irreversible, based on the embedding mechanism.

3.1 Reversible data hiding (RDH):

Reversible data hiding (RDH) techniques emphasize the fact that the original image can be restored after data hiding, which means that the cover image is temporarily damaged after embedding.[14] Therefore, image that requires very detailed information uses reversible data hiding, for example, blueprints, medical, and military applications. However, to preserve the reversibility of the stego image, the embedding rate must be reduced or additional information must be provided to reinstate the cover image[15]. Generally, the complexity associated with using the reversible data hiding method is larger than the complexity associated with the irreversible data hiding process, and the decoding process of reversible data hiding requires the simultaneous retrieval of hidden data and the cover image recovery[14]. Over time, several researchers have looked into methods of reversible data hiding. Yan-Hong Chen et al. proposed a method of adaptive reversible data hiding in 2021 based on AMBTC and quantization-level difference.The experimental results show that this method has Av. PSNR and Av.embedding capacity of 31.54 dB and 359,272 bits, respectively, for 512*512 images[16]. In 2019, Xiatian Wu et al. presented partially reversible steganography based on AMBTC. By using the polynomial-based secret image sharing (SIS) under GF(2^8), a hidden image is divided into 'n' noise-like shares. To effectively manage the shares, parity bits are used to conceal them within the AMBTC cover image, and n relevant stego images are created. The embedding rate for this technique is ¼ bpp.[17]. In 2015, Tai-Yuan Tu et al. offered reversible data hiding with a high payload for Vector Quantization (VQ) compressed code index centered on referred frequency. The experimental results of this method are performed on trained images (used for the training process) and non trained images (used for testing).According to the results, trained images have the capacity, cost, and net capacity of 16384, 6722.8, and 9661.2 respectively for codebook size 512, while non trained images have a capacity, cost, and net capacity of 16384, 12618, 3766 respectively, for codebook size 512. And for codebook size 1024, trained images have the capacity, cost, and net capacity of 16384, 6523, 9261 respectively, while non trained images have the capacity, cost, and net capacity of 16384, 12579.33, and 3804.66 respectively[18]. In 2019, Hsiang-Ying wang et al. proposed Reversible data hiding using AMBTC and chaotic encryption for increased security. The experimental results demonstrated that this method has Av. PSNR of 31.265dB and attains Av. Payload of 22451 bits, embedding capacity of 2.04bpp and efficiency of 4.8% for 512*512 images. [14].

3.2 Irreversible data hiding (IRDH):

Irreversible data hiding (IRDH) approaches provide the benefit of greater payload size and quicker decoding speed compared with strategies for reversible data hiding[19]. It allows the hidden data to be extracted from the Stego image, but the original cover image cannot be

recovered. It permanently damages the host media, the cover image loses its originality as soon as the secret message is inserted into it[14]. The stego/marked image cannot be returned to its initial condition using the irreversible data-concealing approach. It doesn't necessitate the use of additional data to recover and extract the information. LSB, EMD, and PVD are the three most common techniques for irreversible data hiding[20].

Least significant bit(LSB) substitution is the simplest method of information hiding in irreversible categories. This technique simply replaces the LSB of the cover image pixel with a secret bit to be embedded. As we replace more LSBs with secret bits, the capacity of this method increases[19]. LSB substitution technology can be subdivided into simple LSB replacement, LSB replacement by Fibonacci decomposition, LSB replacement by prime decomposition, and natural number decomposition LSB substitution[1][21].

The Exploiting modification direction(EMD) approach is block-wise data hiding. It embeds the (2x+1)-array digit data into x steganography pixels by modifying no more than one-pixel value ±1 at most in this set of x pixels and leaves the rest unaltered[22]. The EMD provides good stego image quality because it reduces the number of pixels that need to be changed for data embedding. However, it has a lower embedding capacity than LSB. The Generalized Exploiting Modification Direction(GEMD), Sparse modified signed digit(SMSD), and Enhanced modified signed digit(EMSD) algos improve the payload of EMD[19][23][24].

The Pixel value differencing(PVD)method embeds secret data by manipulating the difference in pixel values between two adjacent pixels. The difference between these two neighboring pixel pairs determines the total number of secret bits[25]. Basic PVD, Multi-directional(MD), Multi-pixel differencing(MPD), side matching, and overlapping pixel value differencing(OPVD)are some methods in the PVD algorithm[26].

To improve the efficiency and capacity of a data-hiding algorithm, any of two or all three techniques (LSB, PVD, and EMD) can be combined.These hybrid techniques are resistant to both RS and pixel difference histogram (PDH) analysis, and they give greater security and lower distortions [10][19][27].Recently, several researchers have investigated Irreversible data-hiding methods.In 2020 S. Solakproposed a hybrid data-hiding method based on enhanced modified signed digit (EMSD) algorithms and LSB replacement to encode secret data. According to the experimental results, the PSNR value is above 43 dB when embedding secret data of approximately 630k bits, above 37 dB when embedding secret data of 900k bits, and above 31 dB while hiding secret data of 1150k bits[19].S. Singh in 2020 developed a method for data hiding that combines LSB and adaptive pixel value differencing to increase data concealing capacity. In this method, in addition to the horizontal edges, the vertical and diagonal edges are also used to conceal secret data, allowing the concealment of a vast amount of data. Based on the findings of the experiments, this approach has an average PSNR of 33.88 dB and an average bit capacity of 139224[27]. In 2017 S. yuan Shen et al. introduced a data-concealing technique that takes human visual sensitivity into account. This method enhances the exploitation modification direction (EMD) in modulus operation. According to the experimental findings, this approach has an average PSNR of 39.165 and an average capacity of 459031 for 512*512 grayscale test images[22]

Table 1: Comparative analysis of RDH and IRDH techniques.

Technique	Algorithms	Av. PSNR(dB)	Av.Embedding capacity(bits) /Av.Embedding rate(bpp)
RDH Tech.	[14]	31.265	22451 bits
	[15]	(a) 53.91	786432 bits
		(b) 52.47	
		(c) 52.48	
	[16]	31.54	359272 bits
	[17]	24.6	¼ bpp
	[18]	-	16384 bits

IRDH Tech.	[19]	(a) 37	900k bits
		(b) 43	630k bits
	[20]	(a) 54.594	121792 bits
		(b) 53.989	128712 bits
	[22]	39.165	459031 bits
	[23]	51.86	1.19 bpp
	[24]	47.90	1.42 bpp
	[25]	30.79	203198 bits
	[26]	53.508	851888 bits
	[27]	33.88	139224 bits

4. DATA HIDING IN IMAGES(IMAGE STEGANOGRAPHY) BASED ON DATA HIDING DOMAINS:

Besides reversible and irreversible data hiding approaches, data concealing can be classed into frequency or transform domain, spatial domain, and compression domains according to data hiding domains[27].

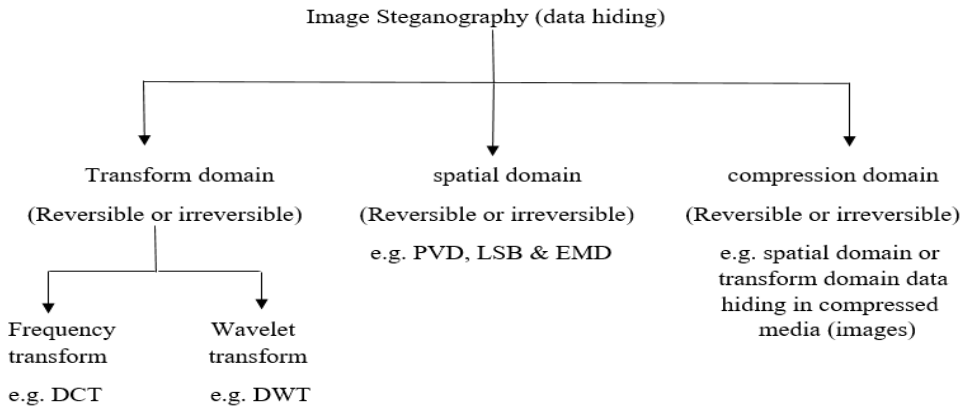

Figure 2: Image steganography techniques

4.1 Data hiding through spatial domain approaches:

To embed information, spatial domain approaches directly operate on image pixels.This means that a few pixel values of the cover image are modified for encoding the message bits. The most widely used algorithms in the spatial domain are the PVD, LSB & EMD[15][19]. In 2021 M. Sahu et al. proposed the idea of the shadow image, which is primarily a copy of the cover image (CI) that is created by adding and subtracting simple logic to the pixels of the shadow image. This spatial domain RDH technique has a large capacity and produces better stego images (SI) quality. The three different SIs produced by this procedure result in three different SSIM and PSNR values. With values of 52.47, 53.91, and 52.48 for PSNR1, PSNR2, and PSNR3, and 0.9974, 0.9981, and 0.9974 for SSIM1, SSIM2, and SSIM3, this method can embed 786432 bits[15].

4.2 Data hiding through transform domain approaches:

In transform domain steganography, the image is first changed from a spatial domain to some other domain and then the secret information is embedded in it.This can be either frequency transform domain steganography or wavelet transform domain steganography.

In Wavelet Transform-based steganography approaches, the original image is transformed into frequency and temporal representation, and then the wavelet (time-frequency) coefficients of the original image are modified to insert the secret information.The most widely used algorithms in the wavelet transform domain areDiscrete Wavelet Transform (DWT), Integer Wavelet transform (IWT),etc[9][28]. Frequency transform domain approaches work with an image's frequency only. It changes the cover picture into a frequency form and the data is then embedded in the frequency

coefficients. The most frequently employed methods are theDiscrete *Fourier Transform (DFT),* Discrete Cosine Transform (DCT),*etc.*based on this [29]. H. Zhang et al. in 2019 presented a technique for hiding data that uses integer wavelet transform and multidirectional line coding. In this technique,by using haar-IWT on the cover image, the first four wavelet subbands were acquired, and the subbands were then separated into 3*3 nonoverlapping coefficient blocks. Following that, the multidirectional line coding (MDLE) approach was used for each coefficient block, with the eight surrounding coefficients of the block being altered for embedding secret information. This approach yields PSNR and embedding capacities of 50.75 dB and 478868 bits, respectively[28]. In 2014 Y. K. Lin et al. proposed a steganographic strategy based on various DCT coefficients of an image.This technique applies DCT using integer mapping, allowing the picture retrieved from the modified coefficients to be translated back to the accurate data hidden coefficients. The outcomes demonstrate that this technique achieves an average PSNR and embedding capacity of 43.99 dB and 455306 bits, respectively[29].

4.3 Data hiding through compression domain approaches:

In comparison to the transform domain approaches, spatial domain methods have the advantage of high embedding capacity and are fast because there is no image transformation but the disadvantage of compression noise and filtering attacks[28]. However, both schemes mentioned above are based on the raw image format and not a compressed image format, which can raise suspicions from invaders because most digital images exchanged over the internet are in a compressed format[25]. Therefore, to overcome this problem and to save the cost of image storage and transmission, as well as to efficiently transfer multimedia data over the internet, data are hidden in a compressed domain [16][17][18]. In the case of the compression domain data hiding method, the cover image is compressed through various compression algorithms, and then by either the spatial domain algorithms or the frequency domain algorithms, the confidential data is encapsulated.In 2019 R. Kumar et al. proposed a method of data hiding in AMBTC compressed images using hamming distance and pixel value differencing methods. Results show that this method has Av. PSNR and capacity of 30.79 and 203198 bits, respectively, for 512*512 grayscale images [25]

Table 2: Comparative analysis of Spatial domain, transform domain, and compression domain steganography.

Technique		Algorithms	Av.PSNR (dB)	Av.Embedding capacity (bits) / Embedding rate (bpp)	Security	Computation cost & computational complexity
Spatial domain		[10]	(a) 40.44	2368750 bits	moderate	Less
			(b) 39.29	2496419 bits		
		[15]	(a) 52.47	786432 bits		
			(b) 53.91			
			(c) 52.48			
		[19]	(a) 37	900k bits		
			(b) 43	630k bits		
Transform domain	Frequency transform	[29]	43.99	455306 bits	High	High
	Wavelet transform	[9]	55.53	-		
		[28]	50.75	478868 bits		
Compression Domain		[5]	32.8568	120000 bits	highest	Depends on compression & data hiding technique. (High if they
		[16]	31.54	359272 bits		
		[17]	24.6	¼ bpp		

					are transformed domain-based and Less if
	[18]	-	16384 bits		
	[25]	30.79	203198 bits		they are spatial domain based)

5. CONCLUSION

This paper presents a study in the area of data hiding. The basic methods of data hiding are reviewed, and the following conclusions are drawn:

1. Cryptography and steganography are methods for hiding information in such a way that the existence of the hidden message cannot be visualized. Several researchers are working to improve the efficiency of algorithms in this field.
2. To increase the efficiency and security of communications, data hiding (or steganography) and cryptography (or encryption) can be integrated into a single unit.
3. The irreversible data hiding method can reach an advanced level of data concealment.
4. When the cover picture has no or little value to decoders, or it is not as important as a hidden message or slight distortion is acceptable, and the primary goal is covert communication, there is no need for reversible data hiding in such applications.
5. Applications, where both the secret message and the cover image are significant to the receiver, use reversible data hiding.
6. Methods for hiding data in the spatial domain are quick and have a high embedding capacity since they directly operate on image pixels and there is no need for image transformation. But they have the drawbacks of filtering attacks and compression noise.
7. To improve the efficiency and capacity of a data-hiding algorithm the spatial domain techniques (LSB, PVD, and EMD) can be combined. These hybrid techniques are resistant to both RS and pixel difference histogram (PDH) analysis.
8. Data hiding is usually performed in the compression domain because most of the images sent over the internet are in a compressed format

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] H. Abdulkudhur Mohammed and N. F. Hameed Al Saffar, "LSB based image steganography using McEliece cryptosystem," Mater. Today Proc., no. xxxx, 2021, doi: 10.1016/j.matpr.2021.07.182.

[2] A. C. Ã, J. Condell, K. Curran, and P. M. Kevitt, "Digital image steganography : Survey and analysis of current methods," Signal Processing, vol. 90, no. 3, pp. 727–752, 2010, doi: 10.1016/j.sigpro.2009.08.010.

[3] O. F. Abdelwahab, A. I. Hussein, H. F. A. Hamed, H. M. Kelash, and A. A. M. Khalaf, "Efficient Combination of RSA Cryptography, Lossy, and Lossless Compression Steganography Techniques to Hide Data," Procedia Comput. Sci., vol. 182, pp. 5–12, 2021, doi: 10.1016/j.procs.2021.02.002.

[4] A. Gambhir, Khushboo, and R. Arya, "Performance analysis and implementation of DES Algorithm and RSA Algorithm with image and audio steganography techniques," in Advances in Intelligent Systems and Computing, vol. 810, Springer Verlag, 2018, pp. 1021–1028.

[5] C. Kim, D. Shin, C. N. Yang, and L. Leng, "Hybrid data hiding based on AMBTC using enhanced hamming code," Appl. Sci., vol. 10, no. 15, pp. 1–18, 2020, doi: 10.3390/APP10155336.

[6] M. S. Subhedar and V. H. Mankar, "Current status and key issues in image steganography : A survey," Comput. Sci. Rev., pp. 1–19, 2014, doi: 10.1016/j.cosrev.2014.09.001.

[7] P. Patil, P. Narayankar, D. G. Narayan, and S. M. Meena, "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish," Procedia Comput. Sci., vol. 78, no. December 2015, pp. 617–624, 2016, doi: 10.1016/j.procs.2016.02.108.

[8] R. Abid et al., "An optimised homomorphic CRT-RSA algorithm for secure and efficient communication," Pers. Ubiquitous Comput., 2021, doi: 10.1007/s00779-021-01607-3.

[9] D. Baby, J. Thomas, G. Augustine, E. George, and N. R. Michael, "A novel DWT based image securing method using steganography," Procedia Comput. Sci., vol. 46, no. Icict 2014, pp. 612–618, 2015, doi: 10.1016/j.procs.2015.02.105.

[10] G. Swain, "A Steganographic Method Combining LSB Substitution and PVD in a Block," Procedia Comput. Sci., vol. 85, no. Cms, pp. 39–44, 2016, doi: 10.1016/j.procs.2016.05.174.

[11] M. Li, X. Yuan, H. Chen, and J. Li, "Quaternion Discrete Fourier Transform-Based Color Image Watermarking Method Using Quaternion QR Decomposition," IEEE Access, vol. 8, pp. 72308–72315, 2020, doi: 10.1109/ACCESS.2020.2987914.

[12] Q. Su et al., "New Rapid and Robust Color Image Watermarking Technique in Spatial Domain," IEEE Access, vol. 7, pp. 30398–30409, 2019, doi: 10.1109/ACCESS.2019.2895062.

[13] G. Badshah, S. C. Liew, J. M. Zain, and M. Ali, "Watermark Compression in Medical Image Watermarking Using Lempel-Ziv-Welch

(LZW) Lossless Compression Technique," J. Digit. Imaging, vol. 29, no. 2, pp. 216–225, 2016, doi: 10.1007/s10278-015-9822-4.
[14] H. Y. Wang, H. J. Lin, X. Y. Gao, W. H. Cheng, and Y. Y. Chen, "Reversible AMBTC-Based Data Hiding with Security Improvement by Chaotic Encryption," IEEE Access, vol. 7, no. c, pp. 38337–38347, 2019, doi: 10.1109/ACCESS.2019.2906500.
[15] M. Sahu, N. Padhy, S. S. Gantayat, and A. K. Sahu, Shadow Image Based Reversible Data Hiding Using Addition and Subtraction Logic on the LSB Planes, vol. 22, no. 1. Springer US, 2021.
[16] Y. H. Chen, C. C. Chang, C. C. Lin, and Z. M. Wang, "An adaptive reversible data hiding scheme using ambtc and quantization level difference," Appl. Sci., vol. 11, no. 2, pp. 1–13, 2021, doi: 10.3390/app11020635.
[17] X. Wu and C. N. Yang, "Partial reversible AMBTC-based secret image sharing with steganography," Digit. Signal Process. A Rev. J., vol. 93, pp. 22–33, 2019, doi: 10.1016/j.dsp.2019.06.016.
[18] T. Y. Tu and C. H. Wang, "Reversible data hiding with high payload based on referred frequency for VQ compressed codes index," Signal Processing, vol. 108, pp. 278–287, 2015, doi: 10.1016/j.sigpro.2014.09.021.
[19] S. Solak, "High embedding capacity data hiding technique based on emsd and lsb substitution algorithms," IEEE Access, vol. 8, pp. 166513–166524, 2020, doi: 10.1109/ACCESS.2020.3023197.
[20] Y. H. Lin, C. H. Hsia, B. Y. Chen, and Y. Y. Chen, "Visual IoT security: Data hiding in AMBTC images using block-wise embedding strategy," Sensors (Switzerland), vol. 19, no. 9, pp. 1–17, 2019, doi: 10.3390/s19091974.
[21] B. Datta, K. Dutta, and S. Roy, "Data hiding in virtual bit-plane using efficient Lucas number sequences," 2020.
[22] S. yuan Shen, L. hong Huang, and S. sen Yu, "A novel adaptive data hiding based on improved EMD and interpolation," Multimed. Tools Appl., 2017, doi: 10.1007/s11042-017-4905-5.
[23] Y. X. Liu, C. N. Yang, Q. D. Sun, S. Y. Wu, S. S. Lin, and Y. S. Chou, "Enhanced embedding capacity for the SMSD-based data-hiding method," Signal Process. Image Commun., vol. 78, no. July, pp. 216–222, 2019, doi: 10.1016/j.image.2019.07.013.
[24] Y. Liu, C. Yang, and Q. Sun, "Enhance embedding capacity of generalized exploiting modification directions in data hiding," IEEE Access, vol. 6, pp. 5374–5378, 2017, doi: 10.1109/ACCESS.2017.2787803.
[25] R. Kumar, D. S. Kim, and K. H. Jung, "Enhanced AMBTC based data hiding method using hamming distance and pixel value differencing," J. Inf. Secur. Appl., vol. 47, pp. 94–103, 2019, doi: 10.1016/j.jisa.2019.04.007.
[26] E. Ansari, "OOPAP and OPVD : Two Innovative Improvements for Hiding Secret Data Into Images," Iran. J. Sci. Technol. Trans. Electr. Eng., vol. 4, 2018, doi: 10.1007/s40998-018-0090-4.
[27] S. Singh, "Adaptive PVD and LSB based high capacity data hiding scheme," Multimed. Tools Appl., vol. 79, no. 25–26, pp. 18815–18837, 2020, doi: 10.1007/s11042-020-08745-5.
[28] H. Zhang and L. Hu, "A data hiding scheme based on multidirectional line encoding and integer wavelet transform," Signal Process. Image Commun., vol. 78, no. July, pp. 331–344, 2019, doi: 10.1016/j.image.2019.07.019.
[29] Y. K. Lin, "A data hiding scheme based upon DCT coefficient modification," Comput. Stand. Interfaces, vol. 36, no. 5, pp. 855–862, 2014, doi: 10.1016/j.csi.2013.12.013.