Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 4 No. 1 (January) (2026)

GSA Driven Distributed Watermarking Technique using 4LSB Substitution

Atiq Ur Rahman
Department of Telecommunication, University of Engineering Technology Mardan, Pakistan Email: atiqurahman1998@gmail.com

Sahib Khan
Department of Telecommunication, University of Engineering Technology Mardan, Pakistan Email: sahib@uetmardan.edu.pk

Abstract

A digital watermark technique is a unique signature used for copyright protection, data integrity, and ownership identification. The digital watermark can be visible, semi-visible, or completely invisible and can be fragile or semi-fragile. The proposed technique presents a gravitational search algorithm based on an invisible watermarking technique that embeds a digital watermark in host images in a distributed manner. The invisibility of the watermark restricts any detection and prediction of the watermark contents and location with the naked eye and keeps it invisible to the human visual system. Hence, make the alteration, removal, or replacement of the watermark difficult. The distributed placement enhances the security of the watermark twofold and limits the complete removal or replacement of the watermark by any random attempts. The proposed distributed watermarking is an optimal solution for embedding watermarks, which applies the gravitational search algorithm, using Newtonian principles, to identify the potential host pixels for watermark embedding. The proposed technique provides average values of hiding capacity of 35%, PSNR of 40 dB or higher, and SSIM of 0.90. The experimental result shows that the embedded watermark remains invisible, keeping the quality of the host image unaffected, and results in a high-quality host image with an embedded watermark.

Keywords: Data Hiding, Gravitational Search Algorithm, Newtonian Principles, Watermarking, Data Integrity

INTRODUCTION

Digital watermarking is the technique of using a type of identifier called a watermark that is secretly implanted in digital information, such as video or images, to identify the ownership of the file or content [1-2]. The main goal of digital watermarking is to establish a persistent link between content and watermark data, which can be recovered later to prove authenticity, image integrity, and ownership. The two main processes of digital watermarking can be expressed as watermark embedding and watermark extraction [3-4]. The watermark is categorized according to various characteristics, such as based on perceptibility, robustness, and on the basis of the embedding domain.

Perceptibility based watermark visible to the human sense are called visible watermark such as TV channel logo and invisible watermark are totally undetectable to human eye, and robustness watermark are mainly three types having characteristic of robustness, which is withstand to common image operation, fragile watermark is corrupted by any small alteration to the host content because more sensitive, and semi-fragile watermark is less sensitive to alliteration and more robust than fragile watermark [5-7].

Domain-based watermarking is called Spatial and Frequency domain watermarking techniques. In the proposed paper spatial domain watermarking used to embed watermark directly into pixel values to modify the image pixel's values such as Least Significant Bit (LSB) which is simple and fast technique but low robustness as compare to frequency domain watermarking in which the host image is firstly transformed frequency domain using different transform techniques such as discrete cosine transform (DCT), discrete wavelet transform (DWT), and discrete Fourier transform (DFT) are high robustness but computational complexity is high [8-9].

Digital watermarking is to enhance the reliability, security and management of data, and to address qualitative and quantitative assessment and ensure image integrity ownership in various fields and industries such as Healthcare and Medical Imaging, The main application of watermarking in medical and health care imaging is to provide these five security services such as integrity, availability and confidentiality to ensure data accuracy, data accessibility and protect data from unauthorized access respectively. Authentication is to provide validity between originator and receiver for transmission, and involvement of non-repudiation is to prove of delivery and sender identity [10].

Intellectual Property Protection (IPP) application, Digital watermarking plays a significant role in intellectual property protection to embed a signature or pattern into digital content to identify the owner, verifying the integrity, enabling the forensic analysis and detecting the copyright infringement, and content base authentication the impact of counterfeiting is a challenging problem, including government, education, research, business, multimedia and many more industries to ensure the authenticity of the intended destination [11]. Therefore, digital watermarking can use a secret message or code to provide an effective deterrent for counterfeiting to ensure content authentication and minimize the problem.

The proposed technique is based on distributed and invisible watermarks using spatial domain embedding techniques called LSB, which have key characteristics such as low computational complexity, high capacity, and fast embedding and extraction process.

LITERATURE REVIEW

The digital watermarking is a technique used to embed unique information, such as an image, video, audio file, or text called a watermark into a host image that is to be protected against abuse [12]. The core purpose of digital watermarking is to provide a security layer of information that remains unaltered throughout the lifecycle when any type of stealing operation, such as editing, transmission, or compression, is applied. There is a vast application of digital watermarking, but the effectiveness of digital watermarking is examined in terms of three fundamentals: imperceptibility, robustness, and capacity.

The origin of watermarking may be traced to the ancient Greeks, who transferred information by modifying and then swapping the position of letters. The first watermark appeared in Italy during the 13th century, but its use rapidly increased across Europe. In the 18th century, watermarks were used for counterfeit-proofing on money and other documents. The first time Emil Hem Brooke used a watermark patent was in 1954, "Identification of sound and like signals". In 1980, to identify their music, Muzak Corporation used an analog audio signal. [13].

The term digital watermarking was first used with the LSB technique in 1994. There is a wide range of applications of digital watermarking, such as copyright protection, source tracking, file integrity, broadcast monitoring, and content management on social networks to ensure security in analog and digital communication [14-15].

After background history and applications, now to discuss classification and methods of digital watermarking:

Type of watermark: visible and invisible watermark.

Robustness: fragile, semi-fragile, and robust watermark

Domain: spatial and frequency domain [16]

Perceptibility: perceptible and imperceptible watermark

Host data: to select digital media such as image, audio, video, or text for embedding watermarking [17].

Data extraction: blind, semi-blind and non-blind watermarking data extraction at the end of the digital watermarking process from watermarked content [18].

Different methods and techniques are discussed to compare with the proposed method at the end of the research.

According to [19], a technique called watermarking spatial domain LSB, considering a host image size of 512x512, and embedding a watermark capacity of 64x64. The concluded result signal quality is superior, and PSNR is 47.6 dB. The speed of operation is fast, and adjustment for color variation is possible.

In [20], the author proposed a watermarking spatial domain LSQB XORING technique taking an image quantum grayscale 255x256 and embedding a grayscale image of size 128x128. The concluded result and PSNR are 46-48 dB. The operation speed is low, and there is no adjustment for color variation.

Ghadi et al. proposed a spatial domain additive embedding technique for both color and grayscale images having size 512x512 and 64x64, respectively [21]. The concluded result robustness is high, and PSNR is between 50.38-47.48 dB. Su and the coauthors implemented the spatial domain additive embedding technique by considering a color image size 512x512 [22] and embedding bit capacity size 32x32. The robustness is medium, and PSNR is between 38.0-36.5 dB

LSB technique [23], the author proposes a spatial domain by considering quantum color having size 256x256 and 512x512, cover image size, and embedding bit capacity quantum binary 128x128 and 256x256. The concluded result robustness is the best one, and PSNR is approximately 58 dB. In [24], the author proposed a watermarking spatial domain LSB technique taking a cover image size of 512x512 and an embedding capacity of 2 bpp. The conclusion of robustness in fragile and image quality is 38.20 to 36.98 dB.

METHODOLOGY

The proposed technique consists of two processes, i.e., the host selection process and watermarking embedding. The distributed watermarking technique identifies the potential host pixels for embedding a watermark within the host image; this process is termed the host selection process. The watermark embedding process uses 4LSB substitution [25] to place the watermark bits in the least significant bits of the selected host pixels of the host image. The 4LSB substitution mechanism ensures that the existence of the watermark is invisible and makes the proposed technique an invisible distributed watermarking. The whole process ensures data integrity as well as security [26]. Each process of the distributed watermarking technique is explained in the upcoming sections in detail below.

Host Pixels Identification using GSA:

The proposed technique uses an optimization algorithm called the Gravitational search algorithm (GSA) that works according to the principle of gravity and motion to classify pixels in different regions in an image for the process of embedding. According to the law of gravity, all particles or agents (pixels) attract each other by the gravitational force. This compels a movement toward heavy mass agents (pixels), which is directly proportional to the product of the mass of the agents (pixels) and inversely proportional to the distance between them. In a detailed discussion, the GSA algorithm, each agent has certain circumstances like position, active, passive, and inertial masses [27].

The GSA took the host image to apply the pre-processing operation of grayscale conversion, denoising to avoid any false host pixel detection, and normalization. The pre-processing makes the host image suitable for the efficient detection of host pixels. After the pre-processing of the GSA algorithm's agents, the pixels of the host images, the initial positions, velocities, and mass values are initialized.

Position corresponds to the location of the pixel mass, which can be represented by x and y coordinates called spatial coordinates, or intensity value, which can vary from 0-255, or representation by texture features, for example, orientation or edge magnitude.

The mass of each agent computing current population fitness; the fitness showing the difference between edges pixel with the neighbor's pixel and in Maximization problem the best(t) and worst(t) are defined.

According to the law of gravitational lighter mass called active gravitational mass attracted by heavy mass called passive mass which inserts a force on active mass in specific condition of timeimage.png, image.png is the gravitational constant should be start from the beginning and to reduce with time to achieve and control search accuracy.

Additionally, to calculate the total force image.png act on pixels in position i in dimension d from pixels' position j, which is randomly weighted sum in dth components, and the acceleration of active pixels' position i is given in an equation 1 and 2 respectively.

$$F_i^d(t) = \sum_{j=1, j\neq i} \quad rand_j F_{ij}^d(t) \tag{1}$$

$$a_i^d(t) = \frac{F_i^d(t)}{M_{ij}(t)} \tag{2}$$

Where $rand_j$ interval **[0, 1]** use this for to randomized characteristic to the search.

The solution to the problems is related to the position of the mass, to calculate position and its velocity to continue the embedding process toward fitness, and to select the maximization (to determine the targeted function's highest possible value).

$$v_i^d(t+1) = rand_i \times v_i^d(t) + a_i^d(t) \tag{3}$$

$$x_i^d(t+1) = x_i^d(t) + v_i^d(t+1) \tag{4}$$

The GSA algorithm results in a binary map that contains the location of all the host pixels to be used for watermark embedding. The complete process of the GSA algorithm is summarized in Figure 1.

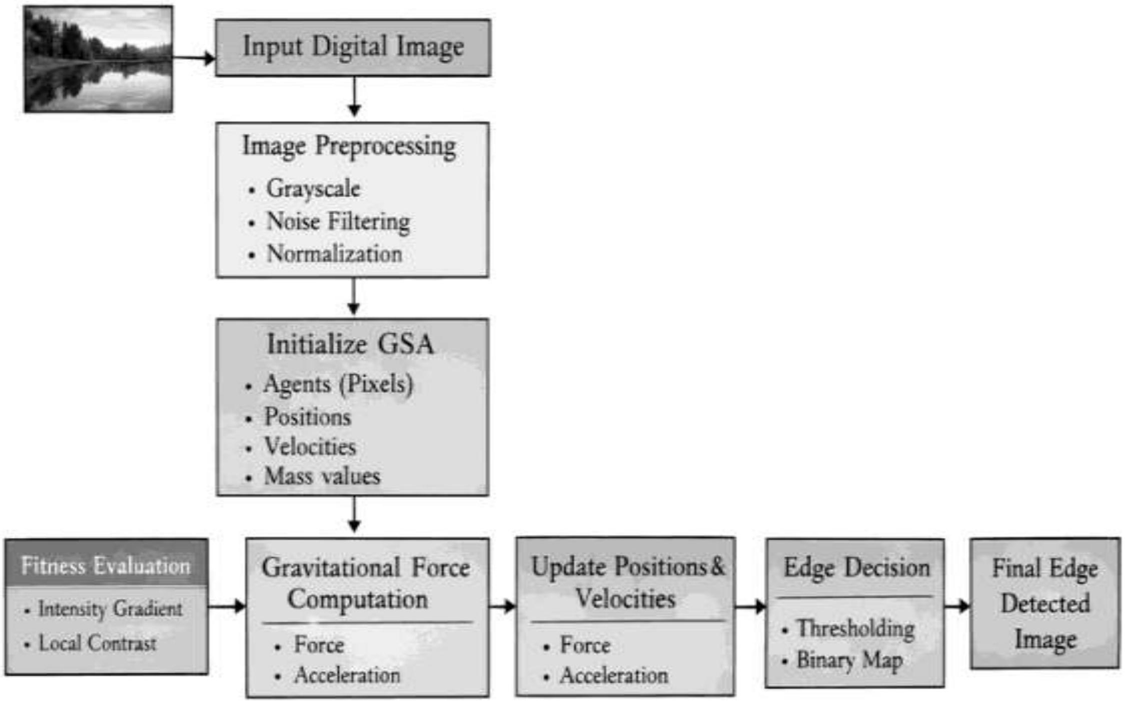


Figure 2: Host pixels identification process using GSA

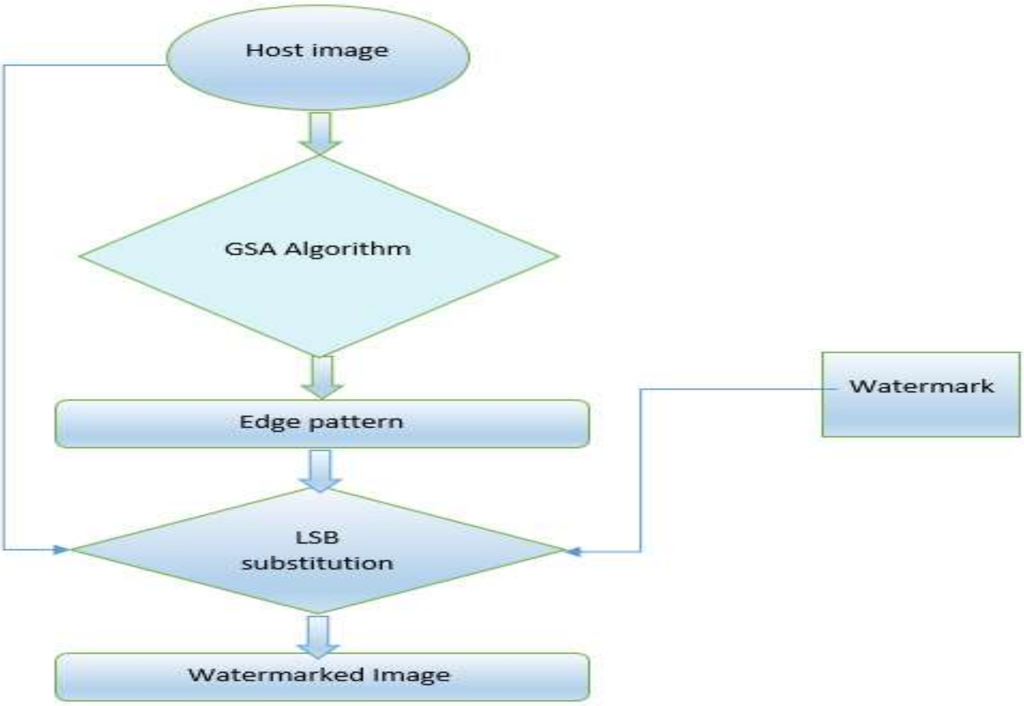


Figure 2: The Proposed Technique

Embedding Process:

The embedding process uses a 4LSB substitution [28] mechanism for embedding the bits of the watermark in the least significant bits of the host pixels of the host image. The embedding process considers each pixel of the host image and checks the binary map whether the pixel is a potential host pixel or not [29]. If the pixel is not a potential host pixel, then it is discarded, and the next pixel is selected and processed accordingly.

If the pixel is a host pixel, the 4LSB substitution mechanism is adopted, and the 4 bits of the watermark are placed in the four least significant bits of the host pixel using the 4LSB technique. Each pixel of the host images is processed in this manner.

The embedding process stops when the whole watermark is placed or embedded in the host image or when all host pixels of the host image are utilized. The whole process results in an image with an embedded watermark.

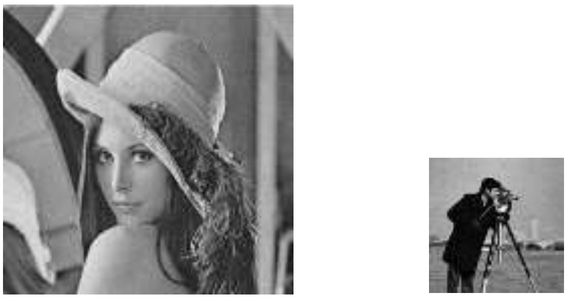
The whole process of GSA driven distributed watermarking techniques is summarized in Figure 2.

RESULTS AND ANALYSIS

The proposed algorithm is applied using Lena as the host image, as given in Figure 3(a), and using a watermark given in Figure 3(b). The host image is initially processed using the GSA algorithm to find the binary map. The parameters of the GSA used for the experimentation are given in Table 1.

Table 1: Parameters and values used for experimentation

PARAMETERS	**VALUES**
Window size (WS)	22
MEAN	0.33
T1	114
T2	140
Beta	6
a	0.34
b	0.34



(a) (b)

Figure 3. The host and watermark a) Host Image, b) Watermark

The GSA, with the parameter values given in Table 1, resulted in a binary map shown in Figure 4.

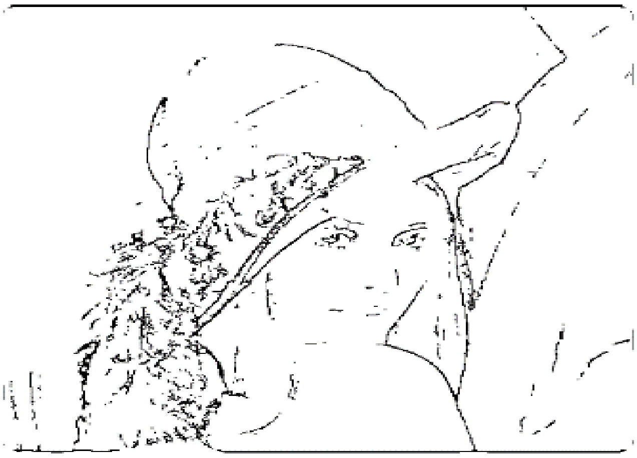


Figure 4. Binary map obtained with GSA

The binary map and the host image are then passed through the embedding process. The watermark given in Figure 3(a) is embedded in the least significant bits of the host pixels of the host image using the 4LSB substitution mechanism. The embedding process resulted in an image, called a watermarked image, with an embedded watermark inside it. The resultant watermarked image is shown in Figure 5.

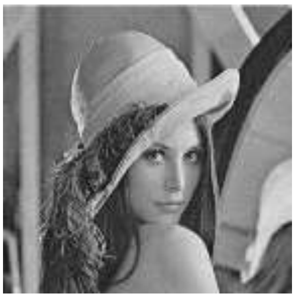


Figure 5. The resulting watermarked image

The resulting image given in Figure 5 shows that the watermark is embedded in an innocent manner, and the existence of the watermark is invisible. Hence, the watermark is not detectable to the human visual system (HVS), nor does it create any sort of distortion to attract the attention of any viewer. The result shows that the visual quality of the watermarked image generated with the proposed technique is the same as that of the original host image.

Checking the quality of the watermarked image qualitatively is not enough to prove the strength of the algorithm. Therefore, the proposed algorithm is also analyzed quantitatively using the evaluation metrics of hiding capacity (HC), peak signal to noise ratio (PSNR), and structure similarity index (SSIM) [30]. The experiment shows that while embedding a watermark in the host image, resulting in a watermarked image given in Figure 5, results in a hiding capacity of 35%, PSNR of 89 dB, and SSIM of almost 0.9908. The result is that the PSNR is higher than a threshold value of 3o dB, which indicates a significant quality of the watermarked image

The proposed technique is also applied to the Coin image as shown in Figure 6. The coin image is used as a host image, while the same Figure 2(b) is used as a watermark for the experimentation. The parameters of the GSA are set according to Table 1. The GSA algorithm resulted in a binary map as given in Figure 7.

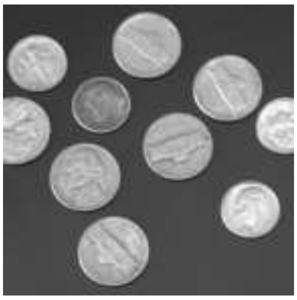


Figure 6. Coin image used as host image

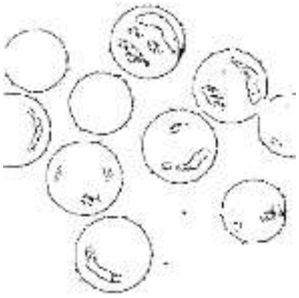


Figure 7. Binary map obtained with GSA using Coin image as a host

The binary map, given in Figure 7, and the host image, given in Figure 6, are used in the embedding process using the 4LSB substitution. The 4LSB substitution mechanism embeds the watermark bits in the host pixels of the host image. The host pixels are identified with the help of the information present in the binary pattern. The embedding process resulted in a watermarked image, shown in Figure 8.

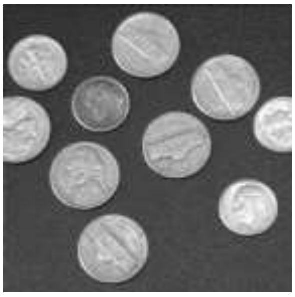


Figure 8. Watermarked image obtained using Coin image as a host

The same evaluation metrics of hiding capacity (HC), peak signal to noise ratio (PSNR), and structure similarity index (SSIM) are used for quantitative analysis of the proposed algorithm using the Coin image as the host. The experimentation shows that while embedding a watermark in the host image, resulting in a watermarked image given in Figure 5, results in a hiding capacity of 35%, PSNR of 95.69 dB, and SSIM of almost 0.9998. The result is that the PSNR is higher than the threshold value of 3o dB, which is a significant quality of the watermarked image.

The results obtained for both the host images show that the proposed technique is an efficient technique that keeps the existence of the watermark invisible, safe, and undetectable. The binary pattern enhances the security of the watermark and ensures the distributed mechanism of the watermark.

CONCLUSION

In conclusion, the proposed distributed watermarking technique is a novel approach to achieve invisible watermarking in an efficient and secure manner. The technique keeps the existence of the watermark innocent and undetectable to viewers. The gravitational search algorithm (GSA) is based on Newtonian principles to calculate the movement of objects using pixel intensity values and detect optimal binary patterns, and hence provide an efficient way of selecting the host pixels. The algorithm achieves a PSNR quite higher than the threshold value of 30dB and provides a hiding capacity of 35%, which enables us to embed a watermark, equal to one third in size of the host image. Hence, the proposed technique is a good technique to be used for secure digital watermarking in the modern era.

REFERENCES

Shih, Frank Y. Digital watermarking and steganography: fundamentals and techniques. CRC press, 2017.

Wang, Zihan, Olivia Byrnes, Hu Wang, Ruoxi Sun, Congbo Ma, Huaming Chen, Qi Wu, and Minhui Xue. "Data hiding with deep learning: A survey unifying digital watermarking and steganography." IEEE Transactions on Computational Social Systems 10, no. 6 (2023): 2985-2999.

Hamamoto, Ippei, and Masaki Kawamura. "Image watermarking technique using embedder and extractor neural networks." IEICE transactions on Information and Systems 102, no. 1 (2019): 19-30.

Gupta, Sunil, Kamal Saluja, Vikas Solanki, Kushwant Kaur, Parveen Singla, and Mohammad Shahid. "Efficient methods for digital image watermarking and information embedding." Measurement: Sensors 24 (2022): 100520.

Yeung, Minerva M., and Fred Mintzer. "An invisible watermarking technique for image verification." In Proceedings of international conference on image processing, vol. 2, pp. 680-683. IEEE, 1997.

Barni, Mauro, Franco Bartolini, and Teddy Furon. "A general framework for robust watermarking security." Signal Processing 83, no. 10 (2003): 2069-2084.

Shehab, Abdulaziz, Mohamed Elhoseny, Khan Muhammad, Arun Kumar Sangaiah, Po Yang, Haojun Huang, and Guolin Hou. "Secure and robust fragile watermarking scheme for medical images." IEEE access 6 (2018): 10269-10278.

Cheung, W. N. "Digital image watermarking in spatial and transform domains." 2000 TENCON proceedings. Intelligent systems and Technologies for the new Millennium (cat. No. 00CH37119) 3 (2000): 374-378.

Dabas, Pooja, and Kavita Khanna. "A study on spatial and transform domain watermarking techniques." International journal of computer applications 71, no. 14 (2013): 38-41.

Cox, Ingemar J., Matthew L. Miller, and Jeffrey A. Bloom. "Watermarking applications and their properties." In Proceedings international conference on information technology: coding and computing (Cat. No. PR00540), pp. 6-10. IEEE, 2000.

Kahng, Andrew B., John Lach, William H. Mangione-Smith, Stefanus Mantik, Igor L. Markov, Miodrag Potkonjak, Paul Tucker, Huijuan Wang, and Gregory Wolfe. "Watermarking techniques for intellectual property protection." In Proceedings of the 35th annual Design Automation Conference, pp. 776-781. 1998.

Gupta, Sunil, Kamal Saluja, Vikas Solanki, Kushwant Kaur, Parveen Singla, and Mohammad Shahid. "Efficient methods for digital image watermarking and information embedding." Measurement: Sensors 24 (2022): 100520.

Laurentius, Frans, and T. Laurentius. Italian Watermarks 1750-1860. Vol. 50. Brill, 2016.

Khan, Sahib, Khalil Khan, Arslan Arif, Mahmoud Hassaballah, Jehad Ali, Qui Thanh Hoai Ta, and Lisu Yu. "A modulo function-based robust asymmetric variable data hiding using DCT." Symmetry 12, no. 10 (2020): 1659.

Khan, Sahib, Khalil Khan, Farman Ali, and Kyung-Sup Kwak. "Forgery detection and localization of modifications at the pixel level." Symmetry 12, no. 1 (2020): 137.

Wahid, Muneeza, Nasir Ahmad, Muhammad Haseeb Zafar, and Sahib Khan. "On combining MD5 for image authentication using LSB substitution in selected pixels." In 2018 International Conference on Engineering and Emerging Technologies (ICEET), pp. 1-6. IEEE, 2018.

Panah, Arezou Soltani, Ron Van Schyndel, Timos Sellis, and Elisa Bertino. "On the properties of non-media digital watermarking: a review of state of the art techniques." IEEE Access 4 (2016): 2670-2704.

Cheema, Adnan Mustafa, Syed Muhammad Adnan, and Zahid Mehmood. "A novel optimized semi-blind scheme for color image watermarking." IEEE Access 8 (2020): 169525-169547.

Bamatraf, Abdullah, Rosziati Ibrahim, and Mohd Najib B. Mohd Salleh. "Digital watermarking algorithm using LSB." In 2010 International Conference on Computer Applications and Industrial Electronics, pp. 155-159. IEEE, 2010.

Abd El-Latif, Ahmed A., Bassem Abd-El-Atty, M. Shamim Hossain, Md Abdur Rahman, Atif Alamri, and Brij B. Gupta. "Efficient quantum information hiding for remote medical image sharing." IEEE Access 6 (2018): 21075-21083.

Ghadi, Musab, Lamri Laouamer, Laurent Nana, and Anca Pascu. "A blind spatial domain-based image watermarking using texture analysis and association rules mining." Multimedia Tools and Applications 78, no. 12 (2019): 15705-15750.

Su, Qingtang, Decheng Liu, Zihan Yuan, Gang Wang, Xiaofeng Zhang, Beijing Chen, and Tao Yao. "New rapid and robust color image watermarking technique in spatial domain." IEEE Access 7 (2019): 30398-30409.

Hu, WenWen, Ri-Gui Zhou, Jia Luo, and BiYing Liu. "LSBs-based quantum color images watermarking algorithm in edge region: W. Hu et al." Quantum Information Processing 18, no. 1 (2019): 16.

Parah, Shabir A., Javaid A. Sheikh, Farhana Ahad, and G. M. Bhat. "High capacity and secure electronic patient record (EPR) embedding in color images for IoT driven healthcare systems." In Internet of things and big data analytics toward next-generation intelligence, pp. 409-437. Cham: Springer International Publishing, 2017.

Khan, Sahib, Muhammad Nawaz Khan, Somia Iqbal, Syed Yaqoob Shah, and Nasir Ahmad. "Implementation of variable tone variable bits gray-scale image stegnography using discrete cosine transform." Journal of Signal and Information Processing 4, no. 4 (2013): 343-350.

Evsutin, Oleg, Anna Melman, and Roman Meshcheryakov. "Digital steganography and watermarking for digital images: A review of current research directions." IEEE Access 8 (2020): 166589-166611.

Rashedi, Esmat, Elaheh Rashedi, and Hossein Nezamabadi-Pour. "A comprehensive survey on gravitational search algorithm." Swarm and evolutionary computation 41 (2018): 141-158.

Khan, Sahib, Muhammad Abeer Irfan, Arslan Arif, Arslan Ali, Zain Anwer Memon, and Aleem Khaliq. "Reversible-enhanced stego block chaining image steganography: A highly efficient data hiding technique." Canadian Journal of Electrical and Computer Engineering 43, no. 2 (2020): 66-72.

Kuang, Xin, Wang An Ling, Li Shi Ke, Guo Lei, Pang Jian Ping, Liu Zhi Yue, and Liu Fu Ping. "Watermark embedding and extraction based on LSB and four-step phase shift method." In Proceedings of the 2019 7th International Conference on Information Technology: IoT and Smart City, pp. 243-247. 2019.

Rajput, Shyam Singh, Bhaskar Mondal, and Farheen Qamar Warsi. "A robust watermarking scheme via optimization-based image reconstruction technique." Multimedia Tools and Applications 82, no. 16 (2023): 25039-25060.