IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, December 2024

Image Watermark Embedding Method Based on Security Service Secure

Mr. M. Ajaykumar[1], Mr. K. Bharath Prakash[2], Mr. Md. Kamloddin[3], Mr. K. Praneeth Reddy[4]
Assistant Professor, Department of CSE[1]
Students, Department of CSE[2,3,4]
Guru Nanak Institute of Technology, Hyderabad, India

Abstract: *To solve the problem of privacy leakage and response latency in outsourced image watermark embedding in cloud computing, an efficient and privacy-preserving watermark embedding method for outsourced digital images was proposed by introducing edge computing technology. We had proposed a perturbing encryption method with homomorphism to ensure the information security and the correctness of discrete wavelet transformation in the encrypted domain. In addition, the framework was designed to guarantee the safety of singular value decomposition that edge server could not recover the original image matrix. The experimental results show that the proposed method is superior to similar secure watermarking schemes in terms of encryption/decryption time and ciphertext expansion. The proposed method enables the watermarking operation to be performed in an unsafe outsourced environment while achieving a watermarking effect similar to the plaintext equivalent*

Keywords: privacy leakage

I. INTRODUCTION

The development of artificial intelligence and big data has prompted an explosion of information. Every minute, 1.1 million tweets are sent, 684,478 contents are shared on Facebook, 3.2 million queries are searched on Google, and 48h of videos are uploaded to YouTube [1]. The creation and the dissemination of massive multimedia information leads to disputes over digital copyrights. It poses challenges to users with limited storage/computing resources in watermarking processing. Combining digital watermarking technology [2] and cloud computing technology is effective to alleviate these problems.

In recent years, the development of cloud servers with massive storage and powerful computation has made it possible to outsource large-scale data storage and processing. The task of watermark embedding massive images can now be transferred to the cloud, ensuring the user's copyright ownership and decreasing the amount of local computing/storage resources required [3]. However, outsourcing data often involves trade secrets and user sensitive data [4]. Therefore, it is necessary to construct a privacy-preserving outsourcing watermarking scheme that can protect the privacy and security of data while implementing watermark embedding in the cloud.

There are a lot of digital watermarking related work in recent years [5], [8], [9]. In the plaintext domain, digital watermarking is a technology that embeds additional information into the host carrier to prove ownership. This process mainly includes spatial domain watermarking [10], [11] and transformation domain watermarking [12]. To date, many approaches have been developed for secure image watermarking, for example, the method of reversible data hiding (RDH) in the encrypted domain [13]. For example, Zhang [14] segmented image pixels into groups by blocks in the spatial domain, then encrypted them by the bit flip, and finally embedded secret bits into the least significant bits of the host image. To reduce the error rate of information extraction, Hong et al. [15] improved the algorithm in [14] by employing smoothness between each block and implementing a correlation of pixels at the block boundary. However, this improvement had little effect on performance. To facilitate information embedding, a novel embedding framework was proposed by reserving the space before encryption [16], [17]. However, this was not suitable for practical applications because content owners need to perform extra work, except for image encryption. For improved security and embedding rate, Zhang et al. [18] utilized a public key mechanism to encrypt the carrier image and used the homomorphism of encryption technology to embed secret information. Similar methods were found in the literature

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, December 2024

[19]–[22]. These methods were based on a public key mechanism, but suffered from data inflation and high computational complexity. Considering the potential value of different image file formats, some secure RDH schemes have been proposed for JPEG images [23] and 2-dim vector graphics [24], respectively. It is widely accepted that the ciphertext RDH technology can achieve secure watermark embedding. However, robustness has consistently been a major problem for schemes based on secure RDH. In [25], Peng et al. proposed a separable watermarking scheme to improve the robustness of the method. Based on chaotic encryption, Gao and Gao [26] proposed a novel verifiable image encryption, which not only protects the image information but also allows watermark data to be hidden and extracted. However, redundancy loss leads to difficulty in embedding watermarks, as well as the reduction of the capacity to embed watermarks. Yao et al. [27] proposed a scheme for embedding a visible watermark in the bit plane of the encryption domain. However, the visual impact of this watermark on the decrypted image was apparent and caused the use-value of the image to be highly susceptible to destruction. Literature [28] studied the watermark embedding of medical images in the encryption domain based on JPEG-LS, concluding that the watermark could be extracted in both the encryption and plaintext domains.

By contrast, much less research has focused on secure watermarking in the transform domain. However, this method has a better robustness and higher embedding capacity [29]. This is especially true for mixing different transformations, such as the combination of discrete wavelet transformation (DWT) and singular value decomposition (SVD). Presently, the watermarking method that combines DWT and SVD can achieve an acceptable balance between robustness and invisibility under appropriate scaling factors, and it has become a common method of watermarking in the plaintext domain [30]. In summary, securely implementing DWT and SVD is imperative in an untrusted environment. The main challenge of the transform domain watermarking scheme in ciphertext is how to ensure a secure frequency transformation operation while obtaining the same effect as plaintext. Zheng and Huang [31] combined the Paillier cryptosystem [32] to propose a DWT transformation in the encrypted domain. However, their data reduction method presented some consistent pixel ciphertext that resulted in a risk of information leakage. Additionally, the discrete Fourier transform [33] and discrete cosine transform [34] of encrypted signals were studied. Inspired by Zheng and Huang's research [31], Xiang et al. [35] proposed a reversible watermark embedding scheme based on the Paillier cryptosystem and multi-level DWT decomposition in the encrypted domain. However, it was challenging to perform multiplication for the Paillier cryptosystem.

Compared to the ciphertext wavelet transformation, there were few studies on singular value decomposition in the encrypted domain. To design a secure outsourcing watermarking framework based on DWT-SVD that was more robust [29], we advanced the encryption method from the literature [36] to encrypt image data and securely perform DWT. Additionally, a secure singular value decomposition framework was designed to compute outsourced SVD. The cloud server can process a large amount of data, but the transmission time is proportional to the amount of data. This implies that data processing outsourced to the cloud may cause a response delay [37]. To solve this problem, we introduced edge computing technology to propose a lightweight privacy-preserving digital watermarking method for outsourced host images.

II. LITERATURE SURVEY

M. Begum and M. S. Uddin. discussed that Image processing and the internet have made it easier to duplicate, modify, reproduce, and distribute digital images at low cost and with approximately immediate delivery without any degradation of quality. Network technology has been developing and progressing so quickly that it threatens the privacy and security of data. Therefore, content authentication, copyright protection, and protection against duplication play an essential role in facing the challenges of the existing and upcoming threats in maintaining digital information. Digital image watermarking is simply the digital watermarking of an image, which provides an alternative solution for ensuring tamper-resistance, the ownership of intellectual property, and reinforcing the security of multimedia documents. Any digital content, such as images, audio, and videos, can hide data. Digital content can easily be illegally possessed, duplicated, and distributed through a physical transmission medium during communications, information processing, and data storage. Digital image watermarking is a technique in which watermark data is embedded into a multimedia product and, later, is extracted from or detected in the watermarked product. These methods ensure tamper-resistance, authentication, content verification, and integration of the image.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, December 2024

K. M. Hosny, M. M. Darwish, and M. M. Foudaexplained thatZero-watermarking methods provide promising solutions and impressive performance for copyright protection of images without changing the original images. In this project, a novel zero-watermarking method for color images is envisioned. Our envisioned approach is based on multi-channel orthogonal Legendre Fourier moments of fractional orders, referred to as MFrLFMs. In this method, a highly precise Gaussian integration method is utilized to calculate MFrLFMs. Then, based on the selected accurate MFrLFMs moments, a zero-watermark is constructed. Due to their accuracy, geometric invariances, and numerical stability, the proposed MFrLFMs-based zero-watermarking method shows excellent resistance against various attacks. Performed experiments using the proposed watermarking method show the outperformance over existing watermarking algorithms. Fast advancements of communication technologies increased the number of transmitted digital images. Image content protection and preserving the intellectual rights are challenging problems. Copyright protection of digital images is a vital security issue. Watermarking technology of digital images has been extensively studied and used as an emerged powerful copyright protection technologies and authentication of the content of digital images and software protection [1]–[4]. In general, the methods of digital watermarking can be classified into different ways [1], [5]: visible, invisible, blind, semi-blind, non-blind, Fragile, semi-fragile, and robust watermarking.

W. Huan, S. Li, Z. Qian, and X. Zhangexplained Video watermarking on the dual tree-complex wavelet (DT CWT) domain is shown to be effective to offer high robustness. Existing DT CWT video watermarking schemes tend to use all the coefficients on the high-pass sub-bands of the DT CWT domain for watermark embedding and detection, which lack of investigating the correlations among different sub-bands and fail to explore the stable coefficients for robust watermarking. In this project, we propose a novel DT CWT video watermarking scheme by exploring the stable coefficients on joint sub-bands. We first extract a set of candidate coefficients by applying block singular value decomposition (SVD) on the DT CWT domain. Then, we simulate the watermark embedding by modifying the candidate coefficients on each sub-band, from which we identity two pairs of strongly correlated sub-bands termed as the joint sub-bands. The watermark is eventually embedded by modifying the candidate coefficients of the joint sub-bands on a level which is adaptively chosen according to the video resolution. During the watermark detection, we identify and extract a set of stable coefficients from the candidate coefficients of the joint sub-bands to verify the ownership of the video. Extensive experiments demonstrate the advantage of our propose scheme over the latest DT CWT based schemes, which also performs better than the existing non-DT CWT transformed domain video watermarking schemes. The rapid development of high-speed networks makes it convenient to spread digital media content over the internet. People can easily upload and share their digital products (e.g., photographs, music or films) through personal website or social networks. However, these products may be downloaded and illegally redistributed without authorization, which seriously jeopardises the owners' interest. Digital watermarking is one of the main techniques that are developed to protect the copyright of digital media content. It embeds the owner's information or some fingerprints (i.e., watermark) into the digital media content, which can be extracted to identify the ownership or trace the distribution history the digital media content.

III. METHODOLOGY

The systems do not simultaneously support both encrypted keyword search and condition-hiding in practice, which limits the commercial applications of proxy re-encryption in the e-healthcare system. We propose a proxy-invisible condition-hiding proxy re-encryption scheme with keyword search to address the issues of inefficiency and condition privacy in the e-healthcare system.

DISADVANTAGES OF EXISTING SYSTEM:

1. Less Security.
2. Not recover the original image
3. More time-consuming of response.

PROPOSED SYSTEM

The proposed scheme requires that the content owner (CO) encrypts the host and watermark images and uploads the encrypted data to the edge computing server.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, December 2024

After obtaining the ciphertext, the server performs the watermark embedding method by combining the Haar DWT (HDWT) and SVD.

The server then returns the encrypted host image containing the watermark to the authorized user who can then decrypt and obtain the corresponding plaintext of the image containing the watermark.

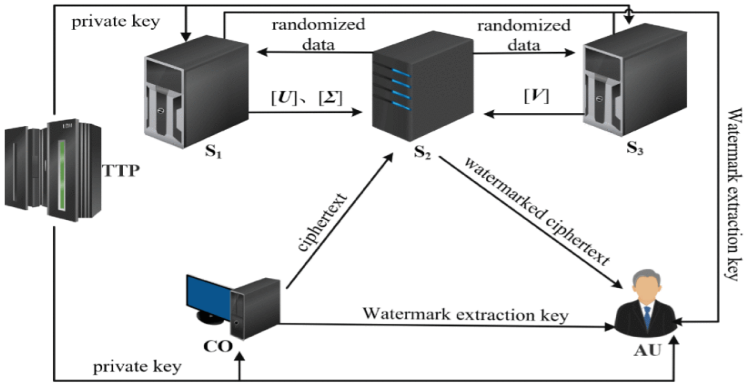
1.The first contribution: A privacy-preserving color image watermarking framework was designed using edge computing technology.

2.The second contribution: An encryption algorithm that is able to perform the HDWT in an encrypted domain was designed.

ADVANTAGES OF PROPOSED SYSTEM:

- High security.
- The watermarking operation to be performed in an unsafe outsourced environment while achieving a watermarking effect similar to the plaintext equivalent

SYSTEM ARCHITECTURE:



MODULES:

User Interface Design: In this module we design the windows for the project. In this module mainly we are focusing the login design page with the Partial knowledge information. Application Users need to view the application they need to login through the User Interface GUI is the media to connect User and Media Database and login screen where user can input his/her user name, password and password will check in database, if that will be a valid username and password then he/she can access the database.

Admin: In this project the admin was done handling the data centers.

Admin was having following operations.

a. Login

b. Add data center regarding different data service providers.

c. Respond (Accept/decline) to customer data center request.

d. View data centers details.

e. Logout.

Data Centre: In this project data centers will store the store (Hold) the customer's data and each data center will have different costs as well as capacity for storage, transfer, get requests and put requests.

Customer (User): In this project the customers or users will store the data into the cloud across multiple cloud providers.

- A customer was having following operations.
- Registration.
- Login.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, December 2024

- Register for data center.
- Send data center request to admin.
- Store the data into data center.
- View the stored data.
- Get the data from data center.
- View the prices (Cost for service).
- Logout.

Data Allocation and Resource reservation (DAR):DAR (Data Allocation and Resource reservation) is a mechanism in our project to minimize the cost of cloud service across multiple cloud providers.

- Getting the customer requirements when they storing the data.
- Estimate the dominant cost of unit data.
- Finding the minimum cost cloud data center.

Store data in that data center which have a minimum cost.

IV. IMPLEMENTATION

Public key encryption:

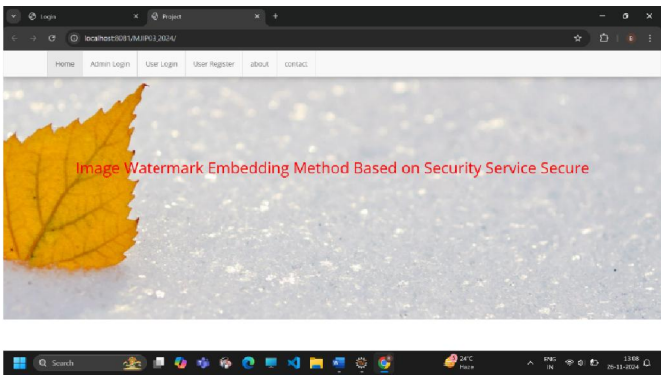
Traditional approaches for image watermarking use public key mechanisms to encrypt the carrier image and employ homomorphic encryption to embed secret information. While these methods ensure a degree of security, they suffer from data inflation and high computational complexity, which lead to performance inefficiencies. Furthermore, existing frameworks for outsourced image watermarking face challenges such as privacy leakage and response latency, particularly when implemented without leveraging advanced technologies like edge computing

Haar Discrete Wavelet Transform (HDWT) and Singular Value Decomposition (SVD) based Technique:

The proposed system introduces a privacy-preserving image watermarking framework utilizing edge computing technology. The content owner encrypts both the host and watermark images before uploading them to an edge server. The server performs watermark embedding by combining Haar Discrete Wavelet Transform (HDWT) and Singular Value Decomposition (SVD) in the encrypted domain, ensuring data privacy. The encrypted watermarked image is then returned to the authorized user, who decrypts it to retrieve the final watermarked image. This method addresses computational inefficiencies while preserving privacy and reducing response latency.

V. EXPERIMENTAL RESULTS

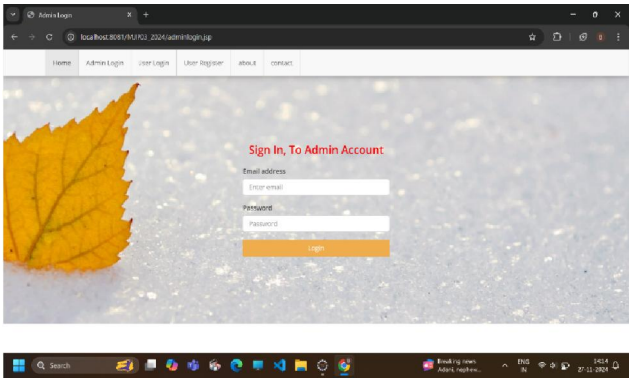
HOME PAGE



EXPLANATION: Upon executing the program and pasting the web address into the browser, the homepage is the initial loaded page. It serves as the primary point of interaction with the website or web application, indicating the initiation of browsing activities.

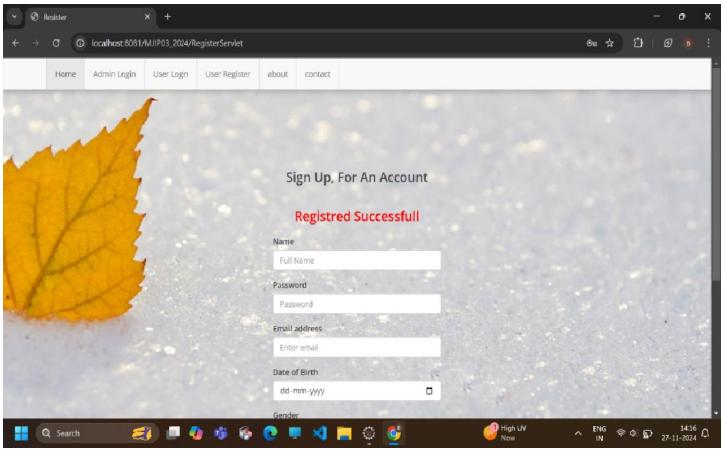
IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, December 2024

ADMIN LOGIN PAGE



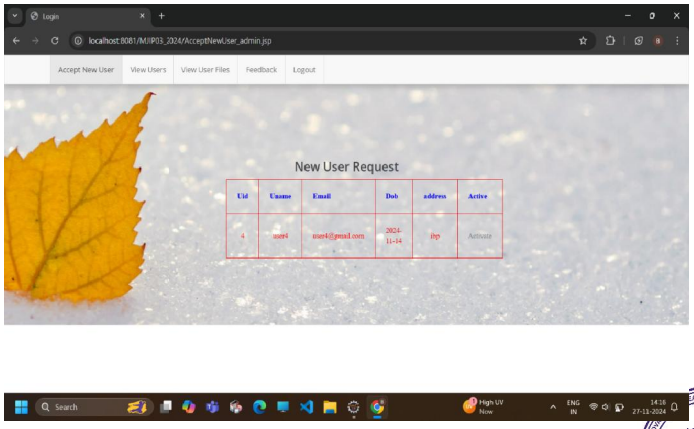
EXPLANATION: Following the click of the login button, the Login page becomes visible, prompting the entry of details. This sequence illustrates the transition from initiating the login process to providing necessary information for authentication. It underscores the procedural nature of user interaction in accessing secured areas of a website or application.

USER REGISTRATION:



EXPLANATION: Before the user start uses his account to encrypt the data he has to register and get the account activated by the admin.

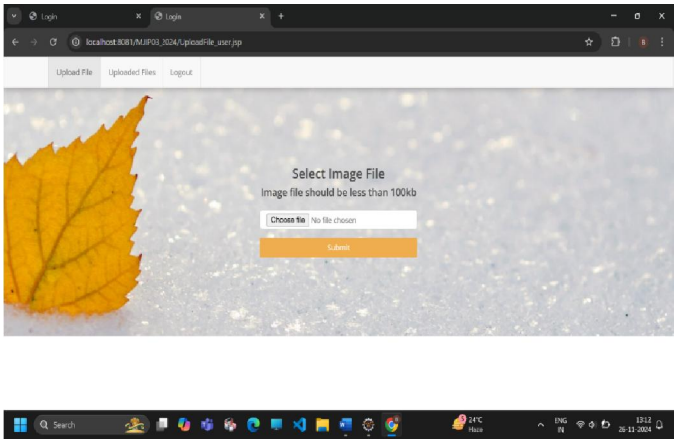
ACCEPT NEW USER :



IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, December 2024

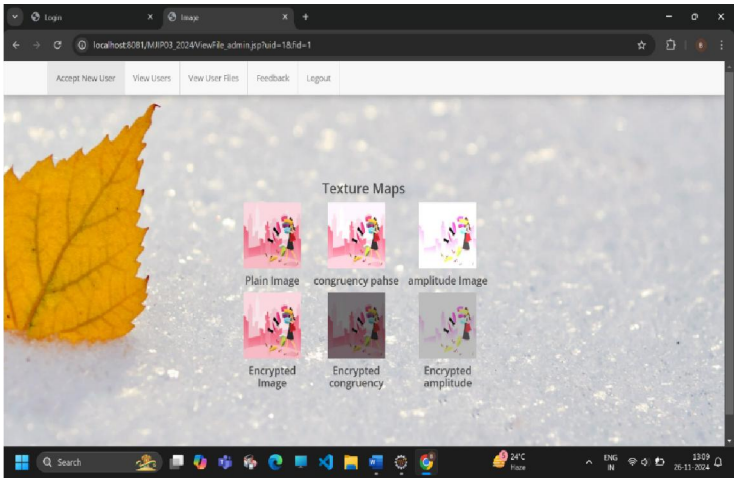
EXPLANATION: Before the admin accepts the user registration no user can login to the account ,to successfully login first the admin needs to activate the account as shown in the above figure. after the account gets activates the user can login to his account , the interface is similar to admin login

UPLOAD FILES



EXPLANATION: After the user has successfully logged into his/her account they can navigate to the upload files page to upload the page and get the image encrypted

FINAL RESULT DETECTION PAGE:



EXPLANATION: After the file is uploaded it goes through different phases and in each phase the image gets encrypted and the images of each of these phases is stored in a file .User and admin have access to view these files

VI. CONCLUSION

In this project, a Haar discrete wavelet transform scheme in the encryption domain was initially proposed. A watermark embedding framework based on edge computing for privacy protection was subsequently proposed, which successfully implements the watermark embedding process of privacy preservation in an insecure outsourcing environment, to achieve an embedding effect similar to that of plaintext domain. Compared with the Paillier cryptosystem commonly used in DWT in the encryption domain, the proposed scheme presents a significant improvement in encryption and decryption rates. Compared with Paillier, the data extension is reduced by about50% in the ciphertext, which makes it feasible for practical applications.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, December 2024

REFERENCES

[1]. Rewarias, "Data privacy in social media platform: Issues and challenges", 2021.
[2]. Begum and M. S. Uddin, "Digital image watermarking techniques: A review", Information, vol. 11, no. 2, pp. 110, Feb. 2020.
[3]. R. Maher and O. A. Nasr, "DropStore: A secure backup system using multi-cloud and fog computing", IEEE Access, vol. 9, pp. 71318-71327, 2021.
[4]. K. M. Hosny, M. M. Darwish and M. M. Fouda, "New color image zero-watermarking using orthogonal multi-channel fractional-order legendre-Fourier moments", IEEE Access, vol. 9, pp. 91209-91219, 2021.
[5]. L.-Y. Hsu and H.-T. Hu, "QDCT-based blind color image watermarking with aid of GWO and DnCNN for performance improvement", IEEE Access, vol. 9, pp. 155138-155152, 2021.
[6]. W. Huan, S. Li, Z. Qian and X. Zhang, "Exploring stable coefficients on joint sub-bands for robust video watermarking in DT CWT domain", IEEE Trans. Circuits Syst. Video Technol., Jun. 2021.
[7]. L. Zhu, X. Luo, Y. Zhang, C. Yang and F. Liu, "Inverse interpolation and its application in robust image steganography", IEEE Trans. Circuits Syst. Video Technol., Aug. 2021.
[8]. P. Yang, Y. Lao and P. Li, "Robust watermarking for deep neural networks via bi-level optimization", Proc. IEEE/CVF Int. Conf. Comput. Vis., pp. 14841-14850, Oct. 2021.
[9]. J. Zhang, D. Chen, J. Liao, W. Zhang, H. Feng, G. Hua, et al., "Deep model intellectual property protection via deep watermarking", IEEE Trans. Pattern Anal. Mach. Intell., Mar. 2021.
[10]. M. Xiao, X. Li, Y. Wang, Y. Zhao and R. Ni, "Reversible data hiding based on pairwise embedding and optimal expansion path", Signal Process., vol. 158, pp. 210-218, May 2019.
[11]. M. Ishtiaq, W. Ali, W. Shahzadm, M. A. Jaffar and Y. Nam, "Hybrid predictor based four-phase adaptive reversible watermarking", IEEE Access, vol. 6, pp. 13213-13230, 2018.
[12]. T.-S. Nguyen, C.-C. Chang and X.-Q. Yang, "A reversible image authentication scheme based on fragile watermarking in discrete wavelet transform domain", AEU-Int. J. Electron. Commun., vol. 70, no. 8, pp. 1055-1061, Aug. 2016.
[13]. Y.-Q. Shi, X. Li, X. Zhang, H.-T. Wu and B. Ma, "Reversible data hiding: Advances in the past two decades", IEEE Access, vol. 4, pp. 3210-3237, 2016.
[14]. X. Zhang, "Reversible data hiding in encrypted image", IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255-258, Apr. 2011.
[15]. W. Hong, T.-S. Chen and H.-Y. Wu, "An improved reversible data hiding in encrypted images using side match", IEEE Signal Process. Lett., vol. 19, no. 4, pp. 199-202, Apr. 2012.
[16]. K. Ma, W. Zhang, X. Zhao, N. Yu and F. Li, "Reversible data hiding in encrypted images by reserving room before encryption", IEEE Trans. Inf. Forensics Security, vol. 8, no. 3, pp. 553-562, Mar. 2013.
[17]. W. Zhang, K. Ma and N. Yu, "Reversibility improved data hiding in encrypted images", Signal Process., vol. 94, pp. 118-127, Jan. 2014.
[18]. X. Zhang, J. Long, Z. Wang and H. Cheng, "Lossless and reversible data hiding in encrypted images with public-key cryptography", IEEE Trans. Circuits Syst. Video Technol., vol. 26, no. 9, pp. 1622-1631, Sep. 2016.
]. T. K. Araghi and A. A. Manaf, "An enhanced hybrid image watermarking scheme for security of medical and non-medical images based on DWT and 2-D SVD", Future Gener. Comput. Syst., vol. 101, pp. 1223-1246, Dec. 2019.
[19]. N. Bisla and P. Chaudhary, "Comparative study of DWT and DWT-SVD image watermarking techniques", Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 3, no. 6, pp. 821-825, 2013.
[20]. P. Zheng and J. Huang, "Discrete wavelet transform and data expansion reduction in homomorphic encrypted domain", IEEE Trans. Image Process., vol. 22, no. 6, pp. 2455-2468, Jun. 2013.
[21]. P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes", Proc. Int. Conf. Theory Appl. Cryptograph. Techn., pp. 223-238, 1999.
[22]. T. Bianchi, A. Piva and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted domain", IEEE Trans. Inf. Forensics Security, vol. 4, no. 1, pp. 86-97, Mar. 2009.
[23] T. Bianchi, A. Piva and M. Barni, "Encrypted domain DCT based on homomorphic cryptosystems", EURASIP J. Inf. Secur., vol. 2009, Dec. 2009.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, December 2024

[24]. S.-J. Xiang, X.-R. Luo and S.-X. Shi, "A novel reversible image watermarking algorithm in homomorphic encrypted domain", Chin. J. Comput., vol. 39, no. 3, pp. 571-581, 2016.
[25]. S. Chen, R. Lu and J. Zhang, "A flexible privacy-preserving framework for singular value decomposition under Internet of Things environment", Proc. IFIP Int. Conf. Trust Manage., pp. 21-37, 2017.