International Journal for Rapid Research in Engineering Technology & Applied Science
Vol VIII Issue VI June 2022
ISSN Online: (2455-4723)

Image Security of Digital Image Watermarking Based on DWT-DCT based

M.tech. Scholar Rina Khande, Assistant Professor & Head Ashish Tiwari
Computer science , Vindhya Institute of Technology & Science Indore (M.P) Country
rinakhande09@gmail.com, ashishtiwari205@gmail.com

ABSTRACT -In this project, two algorithms called Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) in digital image watermarking are compared. Therefore, by this method, the best result is obtained in the LL domain according to DWT, and the best result is obtained in the LL domain by DWT, and the best result is obtained in the LL domain by DWT. Therefore, according to the proposed embedding phase and extraction Mark, our schema embeds logo bits in the low frequency domain. Enhance us with image encryption and image watermarking using HUFFMAN coding. The principle of this process is to recover safety and robustness of the proposed DCT and DWT comparison system. Therefore, compared to other methods, this method can provide higher security accuracy and less data loss rate. The method also focuses on improving the quality after the embedding step and the goal of regaining the watermark after the extraction step. After experiments, it turns out that our proposed method provides safety and high performance with lower computational complexity and good target quality. This work evaluates the performance of watermarked images on MATLAB simulation the evaluates performance will be show in terms of peak signal-to-noise ratio (PSNR) and mean square error (MSE).

I INTRODUCTION

In current years, dynamic chaotic organization has been widely used to propose cryptographic primitives with confused behavior or similar accidental assets. In his groundbreaking work, Shannon barbed out exceptional opportunity for dynamic chaotic graphs in communication. He recognized 2 essential attributes that a good data encryption system should have, namely to avoid (resist) numerical attacks: proliferation or confusion. Distribution can propagate changes to the entire encrypted data, while fabrication can hide connection among original data or encrypted data. In recent years, dynamic chaotic arrangement has been widely used to design cryptographic primitives with chaotic behavior and randomness. Like attributes. In his groundbreaking work, Shannon pointed out exceptional opportunity for dynamic chaotic graphs in communication. He identified 2 basic attributes that a good data encryption system should have, namely to avoid (resist) statistical attacks: proliferation or uncertainty. Diffusion can propagate changes to the entire encrypted data, while fabrication can hide connection among original data or encrypted data. Displacement of rearrangement of objects is the simplest method of diffusion or replacement that is, replacing an object with another object, which is simplest type of perplexity. The dependable use of permutation or replacement methods based on dynamic chaotic systems is the basis of deep cryptography.

Data shooting is a set of method used to place protected data in host media (such as images) with minimal degradation of host performance as well as methods for subsequent extraction of secure data. For exemplar, steganography can be named. Steganography is such a pro-security innovation where secret data is entrenched in cover. Reversible data that hides inserts information bits by changing host signal, but after remove integrated information, original host signal can be restored accurately (losslessly). Sometimes terms like distortion-free, reversible, loss-free or erasable watermark are used as synonyms for reversible watermarks.

In most function, small distortions due to data implant are frequently tolerable. though, ability to restore accurate original images is an ideal feature in many areas, such as law, medicine, and military imaging. After the hiding process, the covered object resembles the invisible object. Therefore, hidden (hidden information) and cryptography (protection of information) are completely different. The discovery process for steganography is called steganalysis. Some applications of steganography include ownership protection, identity verification, air traffic monitoring, medical applications, etc. Steganography is a technique of hiding secret letters in cover image to produce a stealth image.

The recipient of invisible image can use his knowledge of particular occultation method used to recover the hidden text from invisible image. Information concealment is a rapidly evolving technology in the field of information refuge or has attracted much attention from manufacturing or academia. It includes 2 main branches: digital watermarking and steganography with password. The carriers of steganography can be images, text, audio or video. Unauthorized persons can easily destroy multimedia data via Internet. Therefore, it is important to be able to transfer data in secret. In steganography, arrangement of

secret message does not change, but it is hidden in cover image so that it cannot be seen.

For example, a message in an encryption text may cause distrust on part of receiver, while an "invisible" message fashioned by a hidden technique will not. In other words, steganography can prevent inadvertent recipients from wondering if the data exists. Steganography software effectively hides information in images, video, audio or text files. The most commonly used steganography techniques are the least effective. The main purpose of steganography is to communicate securely in a way so that the observer cannot see the real message. The system uses controlled contrast enhancement (CCE) and Haar integer wavelet transformation (IWT) to propose a new RDH scheme.

The term watermark is usually related to hidden information or steganography. These three areas have many technologies or home. Their difference depends on design concept or detailed application. Information hiding is a general term for a choice of purpose, including not only data implant but also confidentiality of information. Consequently, term "hidden information" usually covers steganography or watermarking. Stealth is art of hiding information. One of the distinctions among steganography or watermarking is that watermarks usually contain ownership in sequence, while steganography is used to secretly converse among 2 or more parties.

Watermark belongs to the information area. In the last ten years, a lot of investigate has been done in this area. Steganography is used for covert statement, while watermark is used for content security, copyright administration, and content authentication or tampering. The existing and recently proposed data shooting technologies are examined in detail. The technologies are classified according to the different domains in the integrated data. Some process is implement in spatial domain, and some technique are execute in the transformation domain.

The term watermark is usually interrelated to hiding information or steganography. These three areas have many technologies or land. Their difference depends on design concept or specific application. Information beating is a common term for various applications, including not only data implant but also confidentiality of information. Then, term "hidden information" usually covers steganography or watermarking. Stealth is the art of hiding information. One of distinction between steganography or watermarking is that watermarks typically carry ownership in turn, while steganography is used to secretly commune among two or more parties.

Watermark belongs to information area. In the last ten years, a lot of research has been done in this area. Steganography is used for covert statement, while watermarking is used for content security, copyright administration, and content confirmation or tampering. The existing and recently proposed data shooting technologies are examined in detail. The technologies are classified according to the different domains in the integrated data. Some technique is realized in spatial domain, or some methods are execute in transformation domain. Digital content has a higher quality or value does not decrease over time. Digital files are easy to modify. A person can paste or remove information in the exact place. In addition, digital contented can be simply transferred over the system or to other locations.

Motivation-Recent developments in digital technology and the Internet have made it easy for people around the world to access digital resources. This exposes digital resources to the threat of downloading and then illegal editing to create the threat of counterfeiting. Unauthorized users sometimes assign the modified content as their own resources for personal benefit. In addition to the possible loss of revenue, these issues often lead to misuse of content against the original intentions of the original owner. Digital watermarking is intended as a potential tool to control unauthorized use of digital resources by implementing a mechanism that protects ownership against unauthorized use. In addition, as ownership protection is always an extremely important consideration for content owners, digital watermarks are now widely used in electronic publications, online newspapers, digital libraries and social networking sites. Although significant progress has been made in digital image watermarking, many challenges, such as the imperceptibility of watermarking and resistance to attack, will still be addressed more effectively. Although watermark schemes are proposed with different considerations, such as security, capacity, content authentication, etc., there are few effective multifunctional schemes. In addition, the most important thing is that digital watermark processing must meet the competing requirements of imperceptibility, security and capacity. This means that a robust solution is required that does not significantly reduce the image quality. This effective watermark scheme allows watermark images to be published in the public domain or the Internet and provided free of charge without the worry of unauthorized use or unrecognizable fake images.

II METHODOLOGY

This work presents a new digital watermarking algorithm based on combination of two transforms: DWT and DCT. Here comparative results for two level, three level and fourth level of DWT are present for both NEA and Cox's additive algorithm. Watermarking is done by altering the wavelets coefficients of carefully selected DWT sub-bands

of a 512 × 512 gray scale host image after required level of DWT decomposition, followed by the application of the DCT transform on the selected sub-bands. A 32×32 gray scale mark image enrolled with a key is transform to DCT and then embedded with the host image for fourth level of DWT. Similarly 64 × 64 and 128 × 128 mark image are used in case of three level and two level of DWT. Here the original host image is used for extracting the mark image,

This approach can access in different resolution levels of image due to the wavelet watermarking and can process in real time. Before embedding the secret key in the image, we are going to crypt it with an asymmetric algorithm. At the reception, only public-private key will be needed to extract and decrypt the secret key to get our image legible. To encrypt the image, we have chosen to work with a symmetric stream cipher and symmetric bloc cipher so we can make a comparison between them. To embed the secret key, we selected a watermarking method based on discrete wavelet transform DWT

Reliable digital image watermarking technology using DCT (Discrete Cosine Transform) changes the coefficients in the frequency range. Compared to our spatial method, this will make small, insignificant changes to the whole image and make the attack stronger. DCT is one of the most commonly used methods in water treatment. Safe digital watermarking via DWT (Discrete Wavelet Transform) • In DWT, the distribution is divided into two parts: frequency and time • The most common part is the edge element of the sign. • The lower part is usually divided into two parts, the lower and the lower frequency. • This process can be performed on a regular basis and is often put into practice on hand.

Module Description

Input Image:-Images are a kind of rectangular response (pixels). Each pixel represents a specific character measurement of the measured dimension. This property may have many, but we usually measure the average size (one value) or the brightness (three values) of the image filtered through red, green, and blue filters. These values are usually replaced by eight integers that give a maximum resolution of 256. We are talking about image resolution: defined by number of pixels or number of light values. Use "imread" command to read image in workspace. This instance reads one of exemplar included in the toolbox, image or stores it in a matrix called I. Inferered from the file "unread", that is, graphic file format is "Tagged Image File Format "(TIFF). Use the "Show" function to display image. You can also view imagery in "Image Viewer" application. The "imtool" function can open Image Viewer purpose, which provides a common environment for viewing images or the theater routine image dispensation tasks. The Image Viewer software present imshow image exhibit functionality, as well as contact to many other tools for moving and viewing images, such as scroll bars, pixel area tools, image information tools, and contrast editing tools .

Preprocessing: Image preprocessing is a term used to manipulate images at lowly level of construct. These operations do not increase the content of image information, but if entropy is a measure of information, it reduces content of image information. The purpose of preprocessing is to recover image data to prevent unnecessary manipulation or to improve certain functions related to further processing and analysis. Image processing can manage image redundancy. The adjacent pixels that correspond to the real one have the same note of the same brightness. If the deformed pixel can be retrieved from the image, the adjacent pixels can be restored to a moderate value. Depending on the size of the pixel barrier used to calculate the brightness of the new pixel, the image preparation method can be divided into several categories. The preliminary step is one step before major task of image processing. The difficulty here is to do some basic work to make the customized image more apposite for work to be done. In this case, there may be an improvement in contrast, noise removal, or identification of areas where a zip code may be present. The purpose of preprocessing is to improve the image data, thereby preventing unnecessary distortion or improving the appearance of certain images. Although the shape has changed, these images are still important for further processing. The function of uigetfile is used to compile images from data. After receiving the introductory image, the pre-process is completed. Because the inserted image is adjusted to 256 X 256 image for processing. Similarly, all images in the dataset are preprocessed. The pre-processed image will have some noise that needs to be removed to process the image further. Image noise is most visible in image areas where the signal level is low (for example, shadow areas or under exposed images).

Image Resize:-In computer graphics or digital image processing, image scaling refers to adjusting the size of digital images. In video knowledge, the expansion of digital substance is called magnification or decision improvement. When scaling a vector graphic image, geometric transformations can be used to scale the graphical primitives that make up the image without reducing the image excellence. When you scale a raster graphics picture, a new image with a advanced or lower pixel count must be produce. In case of reduction of number of pixels (downscaling) this typically fallout in a visible loss of quality. From point of view of digital signal processing, scaling of raster graphics is a two-dimensional

instance of sampling rate conversion, ie. Converting a separate signal from one sampling rate (in this case a local sampling rate) to a different sampling rate.

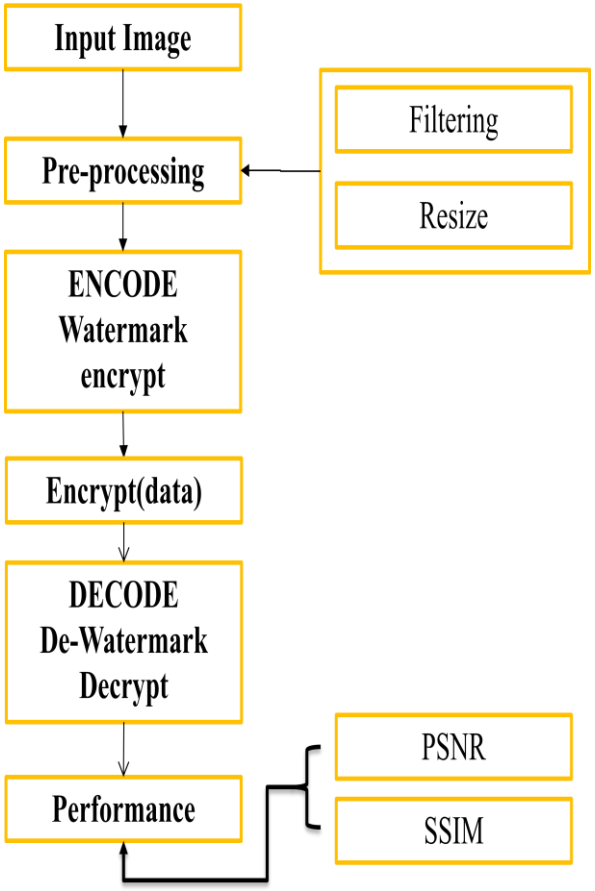

Fig 1 Proposed flow chart

Encode / Decode:-In the last few years, digital watermarking of multimedia contented has become a very active field of research. Watermarking is a very important area with copyright for various electronic documents and media. With the widespread use of images on the Internet, it may sometimes be necessary to use a watermark. Digital watermarking is procedure of processing combined information into digital signals. A watermark is an auxiliary image that overlaps the main image or provides a way to protect the image. It acts as a digital signature that gives the image ownership or realism. Digital watermarking technology is very inspiring in terms of image authentication or attack security. This paper suggests multiple and reversible data hidden in an encrypted image. In planned scheme, an encryption key is used to encrypt original image, and a data slider key is used to integrate other data into the encrypted image. For encrypted images that contain additional data, recipient can still extract the additional data, even if the recipient does not know the contents of image if recipient has only one hiding key. If the recipient has only one encryption key, he can decrypt received data to attain an image corresponding to innovative image, but cannot extract other embedded data. When both encryption and data slider keys are used at same time, by utilizing the spatial connection in the natural image, other entrenched data can be productively extract or original image can be restored entirely.

Performance Estimation

PSNR:

PSNR is easily defined by square error (MSE). If I am given a monochrome m × n image without noise and the average K value of the noise is defined as:

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$
$$= 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right)$$
$$= 20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE)$$

MSE:

The MSE evaluates quality of a predictor (i.e., a function that maps a random input to a example of the value of a accidental variable) or an estimator (i.e., a mathematical purpose that maps a sample of data to an approximation of population parameter, from which data samples). The meaning of MSE varies depending on whether it describes a prediction variable or an estimated variable.If a prediction vector is produce from a example of n data points on all variables, or prediction vector is a vector of experiential principles of envisage inconsistent and is a predicted value (for example, according to least squares fit), then in predictable variable Sample MSE calculated as

$$\mathrm{MSE} = \frac{1}{n}\sum_{i=1}^{n}(Y_i - \hat{Y}_i)^2.$$

MSE can also be calculated on q data point that are not used to estimate model, which may be because they are retained for this principle or because the data is recently attain. In this procedure called cross-validation, MSE is usually called mean square mistake

III MATLAB SIMULATION RESULTS

The MATLAB replication is conceded out in MATLAB 20115 with help of MATLAB image dispensation tool. Figure 1 shows input image with key or remove watermark as output. The images are remove from MATLAB software straight

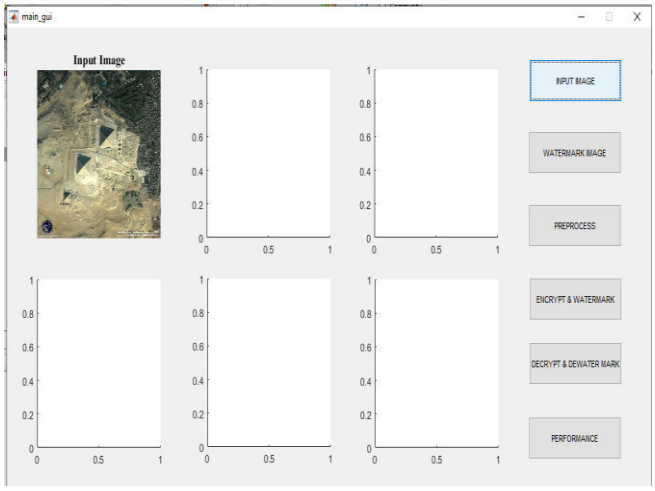

Fig 2 GUI window for input image

Either a digital source based on a source or source can be used. From an application perspective, a source-based code is used to verify your identity or identity. In this case, the sole markup is to notify the owner of the copies similar to the shared image, and also used to identify the weather when the captured image was tampered with. If each distributed copy has a unique label, it can be a location-based marker, which can be used to identify buyers in case of a resale illegal sale. In fact, watermarking will solve the problem of resource verification

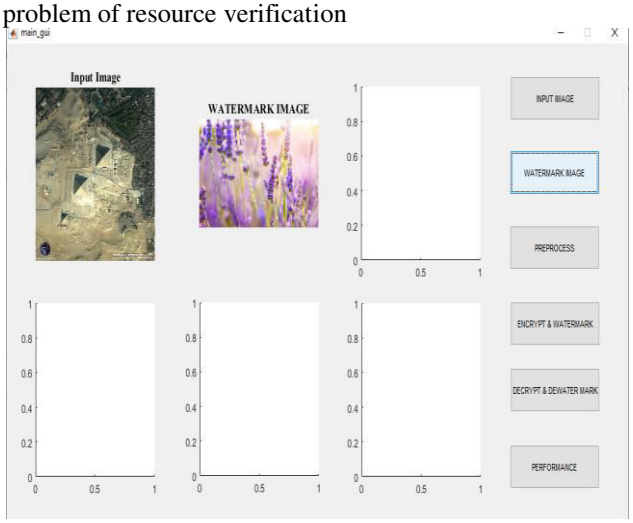

Fig .3 GUI window for water marking image

Image damage will damage or alter the water quality. Changes to the pixel value are not obvious and can be restored as they should. Human vision classifies waterways as strong and fragile

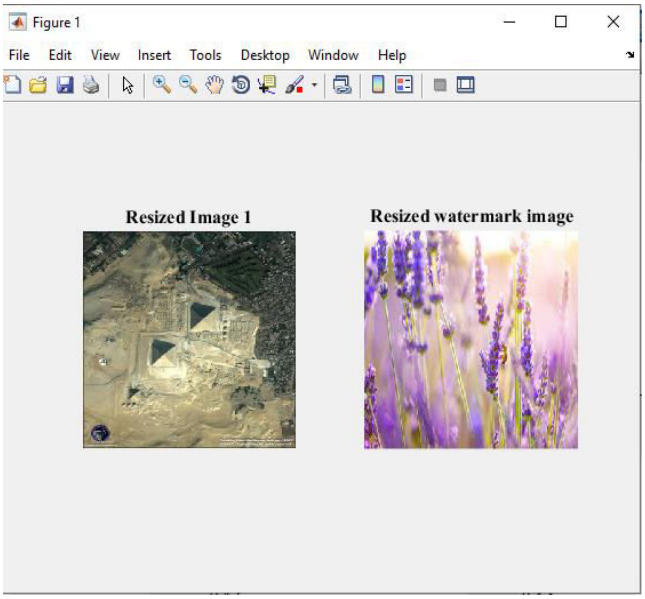

Fig 4 GUI window for resize and water marking resize image

Watermarking and encryption technology are closely linked, but the encryption is not the same as encryption. In a digital watershed system, the water bearing information is included in the original image. The image with the label is sent or saved, and then decoded into parars by the receiver

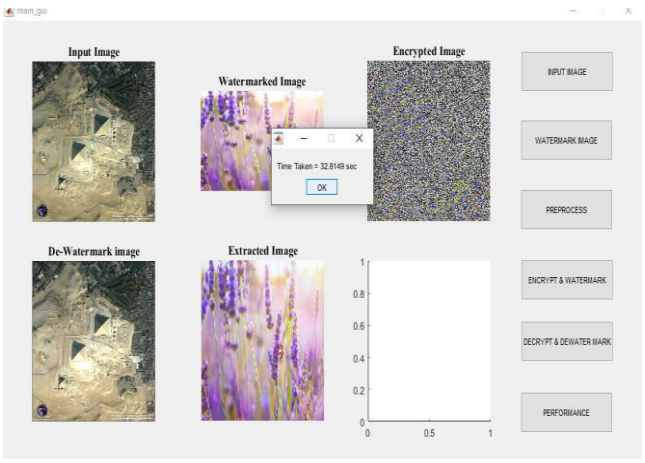

Fig 5 GUI window for resize and water marking resize image encrypted image

In the original message, watermarks are used to protect the data, and these marks are taken at the end of the reception. Therefore, use the code with confidential information to protect them

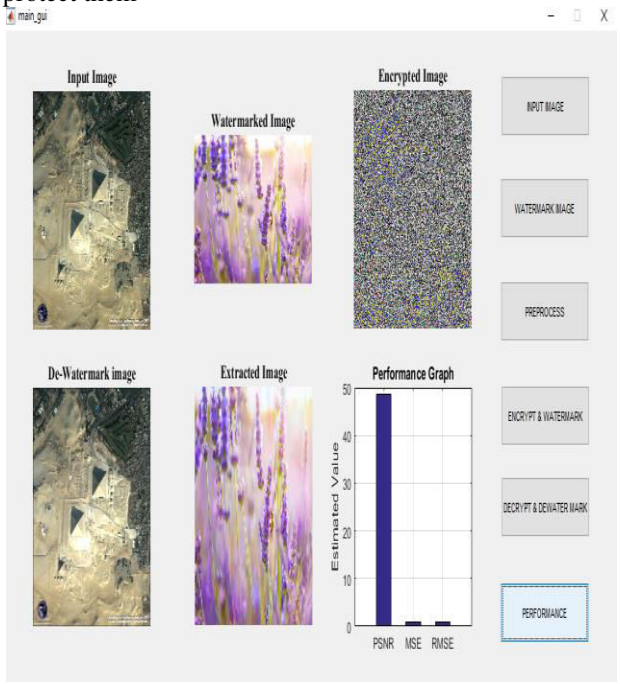

Fig 6 GUI window for resize and water marking resize image de encrypted image

In Cryptography We can use encryption and decryption technology to send and receive secure text and images? Steganography is a technique that uses carrier signals to conceal and publish information. Third, watermarking technology is a technology that hides your information from visual data. Labels include internal verification, copyright protection, copying and manipulation

ENTER THE THREE-DIGIT CODE:3
ENTER THE CODE:3
TIME =
32.8149
Size of the Input Image
No. Of Row 1 = 512
No. Of Col 1 = 512
No. Of Row 2 = 177
No. Of Col 2 = 284

Size of the Output Image
No. Of Row 1 = 300
No. Of Col 1 = 300
No. Of Row 2 = 300
No. Of Col 2 = 300

IV CONCLUSION

The two most common digital watermarks for transformation domain are based on discrete wavelet transformation (DWT) and digital watermark based on discrete cosine transformation (DCT). This article focuses on the technology that combines the two. This article proposes a new embedding algorithm The algorithm evaluates level 2, level 3 and level 4 for DWT. It also describes the comparison results for NEA at these levels and the Cox addition algorithm established under the same environment. Two types of signal-to-noise ratio (PSNR) or correlation are considered to measure imperceptibility and robustness in digital watermarking, respectively. Digital signage is one of the key technologies that can be used in digital rights management systems to locate property, track usage, ensure licensing, prevent illegal copying , and promote content verification. Therefore, a dual security system that uses watermarking and encryption is needed to build an effective DRM system to address IP copyright issues. Digital markers provide an effective and easy way to protect the copyright of digital images. In marker technology, the key to the marker is unique and there is one contract for each marker. Its keys are confidential and only authorized parties can know this, thus eliminating the possibility of illegal use of digital content. The watermarking plan was successfully developed at MATLAB. Perform image processing. The limitation of the watermarking algorithm set is that the processing needs to be done pixel by pixel. In the future, we aim to consider the processing of individual barriers.

REFERENCES

1. Hilkiya Joseph and Bindhu K Rajan Image Security Enhancement using DCT & DWT Watermarking Technique Hilkiya Joseph and Bindhu K Rajan International Conference on Communication and Signal Processing, July 28 - 30, 2020, India
2. Guiliang Gong Kai Zhang Local Blurred Natural Image Restoration Based on Self-Reference Deblurring Generative Adversarial Networks 2019 IEEE International Conference on Signal and Image Processing Applications (ICSIPA) Year: 2019 ISBN: 978-1-7281-3377-5 DOI: 10.1109/ IEEE Kuala Lumpur, Malaysia, Malaysia
3. Heunseung Lim Soohwan Yu Kwanwoo Park Doochun Seo Joonki Paik Texture-Aware Deblurring for Remote Sensing Images Using ℓ0-Based Deblurring and ℓ2-Based Fusion IEEE Journal of Selected Topics in Applied Earth

Observations and Remote Sensing Year: 2020 DOI: 10.1109/IEEE

4. Ryo Tanikawa Takanori Fujisawa Masaaki Ikehara Image restoration based on weighted average of multiple blurred and noisy images 2018 International Workshop on Advanced Image Technology (IWAIT) Year: 2018 ISBN: 978-1-5386-2615-3 DOI: 10.1109/IEEE Chiang Mai, Thailand
5. Jin Liu An Augmented Lagrangian Method for the Patch-based Gaussian Mixture Model In Image Deblurring 2018 IEEE 3rd International Conference on Signal and Image Processing (ICSIP) Year: 2018 ISBN: 978-1-5386-6396-7 DOI: 10.1109/ IEEE Shenzhen, China
6. Wang Manwei Zhu Fuzhen Zhu Bing Bai Yuyang An improved remote sensing image blind deblurring algorithm 2019 3rd International Conference on Electronic Information Technology and Computer Engineering (EITCE) Year: 2019 ISBN: 978-1-7281-3584-7 DOI: 10.1109/IEEE Xiamen, China, China
7. Sheng Liu Yuan Feng Shaobo Zhang Hongzhang Song Shengyong Chen L0 Sparse Regularization-Based Image Blind Deblurring Approach for Solid Waste Image Restoration IEEE Transactions on Industrial Electronics Year: 2019 DOI: 10.1109/ IEEE
8. Fangfang Dong A Fractional-order Differential Based Variational Model for Image Blind Deblurring 2018 IEEE 3rd International Conference on Signal and Image Processing (ICSIP) Year: 2018 ISBN: 978-1-5386-6396-7 DOI: 10.1109/IEEE Shenzhen, China
9. Hongtian Zhao Hua Yang Hang Su Shibao Zheng Natural Image Deblurring Based on Ringing Artifacts Removal via Knowledge-Driven Gradient Distribution Priors IEEE Access Year: 2020 DOI: 10.1109/ IEEE
10. Amreen Kazi S.D. Sawarkar D.J. Pete Image Restoration using Blind Deconvolution 2019 IEEE Pune Section International Conference (PuneCon) Year: 2019 | ISBN: 978-1-7281-1924-3 DOI: 10.1109/IEEE Pune, India, India
11. Haoyuan Yang Xiuqin Su Chunwu Ju Shaobo Wu Efficient Self-Adaptive Image Deblurring Based on Model Parameter Optimization 2018 IEEE 3rd International Conference on Image, Vision and Computing (ICIVC) Year: 2018 ISBN: 978-1-5386-4991-6 DOI: 10.1109/IEEE Chongqing, China
12. Suphongsa Khetkeeree Sompong Liangrocapart Iterative Image Deblurring Algorithm using Complementary Pair of Filters 2019 7th International Electrical Engineering Congress (iEECON) Year: 019 ISBN: 978-1-7281-0729-5 DOI: 10.1109/IEEE Hua Hin, Thailand, Thailand