DOI: http://dx.doi.org/10.26483/ijarcs.v8i9.4969

ISSN No. 0976-5697

Volume 8, No. 9,November-December 2017

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

IMAGE ENCRYPTION STRATEGIES TO ENHANCE SECURITY OF IMAGE: AN EXHAUSTIVE ANALYSIS

Deepakshi Mohal
Department of Computer Engineering and Technology
Guru Nanak Dev University ,Amritsar

Dr. Sandeep Sharma
Department of Computer Engineering and Technology
Guru Nanak Dev University ,Amritsar

Abstract:The accessibility of internet now a days is rapidly increasing that give rise to the problem of protection of digital media and its distribution over the internet. To shield digital media from any unapproved get to advanced watermarking is broadly utilized. It is a path through which a watermark as picture has been implanted and it contains exceptional data. This paper audits different procedures of advanced watermarking, watermarking applications. Additionally some current research in the field of watermarking systems for content reports has been looked into in this paper.

Keywords: watermarking, types of watermarking, spatial watermarking technique, frequency watermarking technique.

1. INTRODUCTION

Watermarking is a procedure through which one can cover up helpful data by the utilization of any digital media. It is a procedure by which one can confirm the verification of the proprietor of a digital media. The digital media can be image, content, video or sound. Watermarking is especially identified with Steganography. Since [1] both the techniques are used to hide the message and allow the transfer process securely. For performing watermarking process, two images are required. The principal image ought to be the first image and the second image ought to be the watermark image. The watermark image is the valuable data which is to be avoided the unapproved creator. The watermark image is valuable for the sender level and additionally for the accepting level. So it ought to be shielded from the unapproved access at the sending level and in addition at the accepting level. Subsequent to performing watermarking process, a third image is acquired which is called Watermarked image. The watermarked image [2]can be distinguished by the approved individual with the utilization of a mystery key. The mystery key is just known to the approved sender and the approved recipient if there should arise an occurrence of a private watermark.

But, if the watermarking procedure is not identified with the security purposes then open watermarks are utilized and the watermarked image is effortlessly accessed by anybody. The entire watermarking procedure ought to take after two stages: installing and extricating. In the implanting procedure, the watermark media is installed or embedded into the first image. Subsequent to inserting, a watermarked image is acquired. In the removed procedure, the watermark is separated from the watermarked image by following an opposite of implanting method. That removed watermark is required at the beneficiary level for acquiring the helpful data (watermark). Watermarking[3] is finished by following a specific technique. The nature of the watermarked image is very relies on the watermarking method utilized. Spatial Domain procedures are utilized for performing watermarking. The watermarking is finished by changing the slightest huge bits of the image in the vast majority of the spatial domain systems. Be that as it may, these systems are not hearty and indistinct. So to obtain great nature of watermarked image, frequency domain methods are utilized. In frequency domain systems, coefficients estimations of the image are changed by following a specific frequency domain strategy. The frequency domain methods are more powerful and subtle than the spatial domain systems. The nature of the watermarked image of the frequency domain strategies is greatly improved than the nature of the watermarked image acquired by spatial domain methods.

Data Transmission [4]through digital media is common now days. As transmission through digital media is increasing so does the attacks. At the time of transmission this data may get affected by noise, or some third party tries to get that data and tamper it. This can be prevented using digital watermarks. The sender who wants to send secret or confidential image to some other person will embed the secret image in another image with the help of a key and send it through the Internet. The receiver will receive that image and extracts the hidden watermark from that image with the help of the shared key.Image security [1] is used effectively to reduce the problems regarding criticality of data represented by the image.Digital watermarking is the method of embedding digitalinformation in any form of multimedia data such as image, audio, video, etc.It is a method of hiding one secretmessage in another message. In earlier days watermarkswere used as trademark or logo for indicating the ownershipof a specific product.But in traditional methods of digital image watermarking, the texture of original image gets distorted more or less.

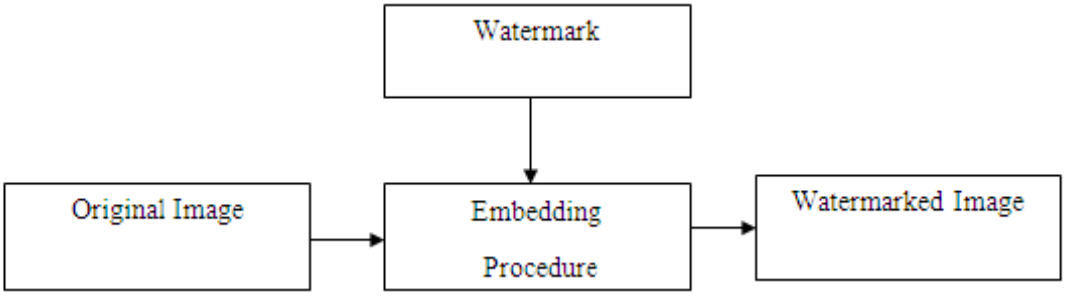

Figure1: Functioning of digital watermarking

2. DOMAINS USED IN DIGITAL WATERMARKING

- Domain associated with space(Spatial)
- Domain associated with Frequency

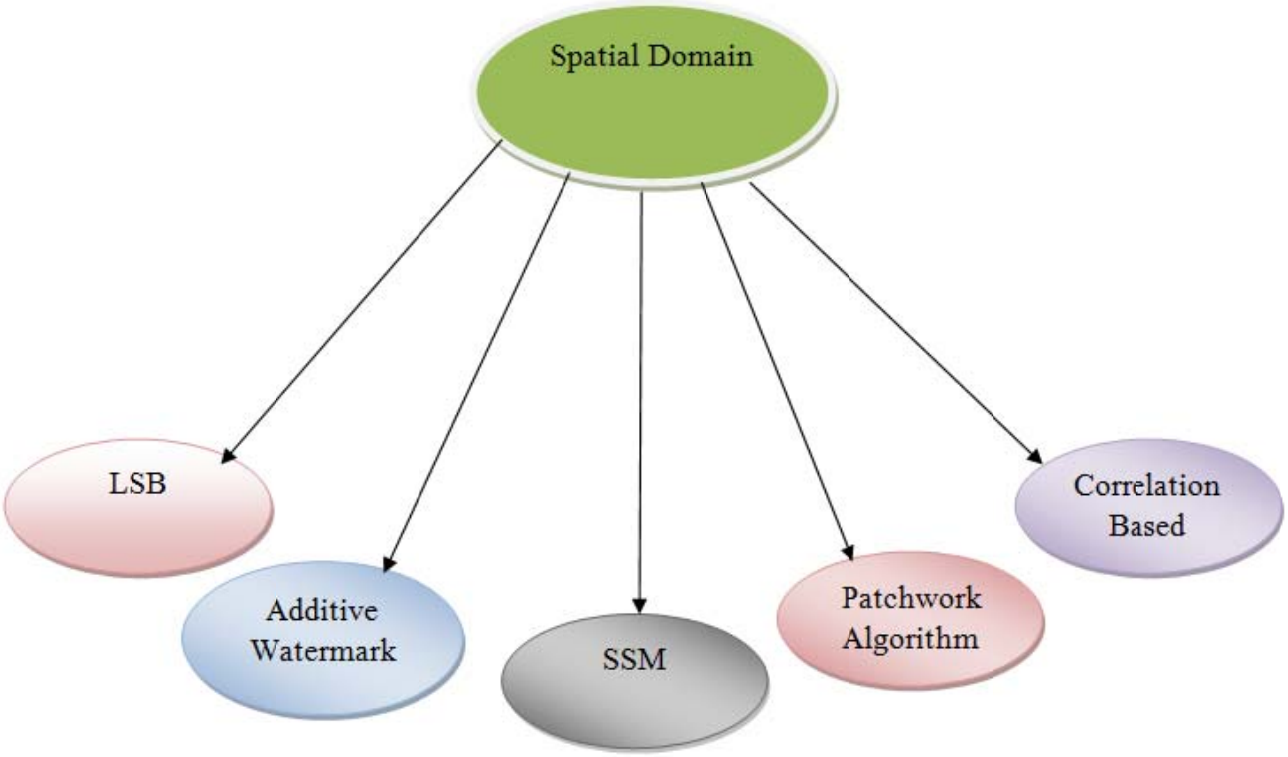

Figure2 : Spatial Domain

- **Space Domain**
  Watermarking[5] strategies in view of spatial space were created first.They are nothing but difficult to actualize and less perplexing. This space encase the message inside the picture specifically. More pace will be used in this case.This space accentuation on altering maybe a couple arbitrarily pick subsets of a picture for straightforwardly stacking the crude information into the pixels.These calculations depend on coordinate installing of watermark into the picture pixels. Some of its primary are as talked about beneath:

➢ **LSB :**
Least Significant Bit[6] is a spatial area system which is an exceptionally basic and straight forward. It requires less investment to install watermark .The watermark is implant into the least significant bits of the first picture. This method has numerous disadvantages, even straightforward assaults can evacuate or crush watermark however at some point it might make due against a portion of the changes. Pixel can likewise be chosen with help of key. Any expansion of commotion and performing lossy pressure can without much of a stretch debase the picture quality or expel or crush or upset watermark. It does not have the essential heartiness. It turns out to be simple for aggressor to change or evacuate watermark.It isvulnerable to trimming, scaling assaults with LSB.

➢ **Additive Watermarking :**
The most clear strategy [7]for installing the watermark in spatial domain is to add pseudo arbitrary clamor example to the power of picture pixels. The clamor flag is generally whole numbers like (- 1, 0, 1) or once in a

while coasting point numbers. To guarantee that the watermark can be distinguished, the commotion is created by a key, with the end goal that the connection between the quantities of various keys will be low.

- **SSM Modulation Based Technique:**
  Spread-spectrum strategies [8] are techniques in which vitality created at least one discrete frequencies is intentionally spread or disseminated in time. SSM based watermarking calculations install data by directly joining the host picture with a little pseudo clamor flag that is tweaked by the inserted watermark.

- **Patchwork Algorithm:**
  Patchwork[9] is a data hiding technique which depends on a pseudorandom, measurable model. Interwoven vaguely embeds a watermark with a specific measurement utilizing a Gaussian distribution. A pseudo arbitrarily choice of two patches is completed where the first is An and the second is B. Fix A picture information is lit up where as that of fix B is obscured. The main disadvantage if this technique is that it hides very small amount of information.

- **Correlation-Based Technique:**
  In this system, a pseudorandom clamor (PN) design says W(x, y) is added to cover picture I(x, y). [10]
  Iw(x, y) = I(x, y) + k*W(x, y)
  Where K speak to the pick up factor, Iw speak to watermarked picture subterranean insect position x, y and I speak to cover picture. Here, on the off chance that we increment the pick up factor at that point in spite of the fact that it expands the strength of watermark yet the nature of the watermarked picture will diminish.But the spatial domain methods provide less resistance to various attacks to image. As a result frequency domainmethods were developed.

- **Frequency Domain**
  In this[11], we use two images(one is the image to be watermarked and another image is on which we place the watermark) should be used for transformation to frequency domain.
  The frequency domain of the two images is added in different proportions and inverse transform of the output is taken to get the watermarked image. This can be done using different transforms techniques which are as follows:

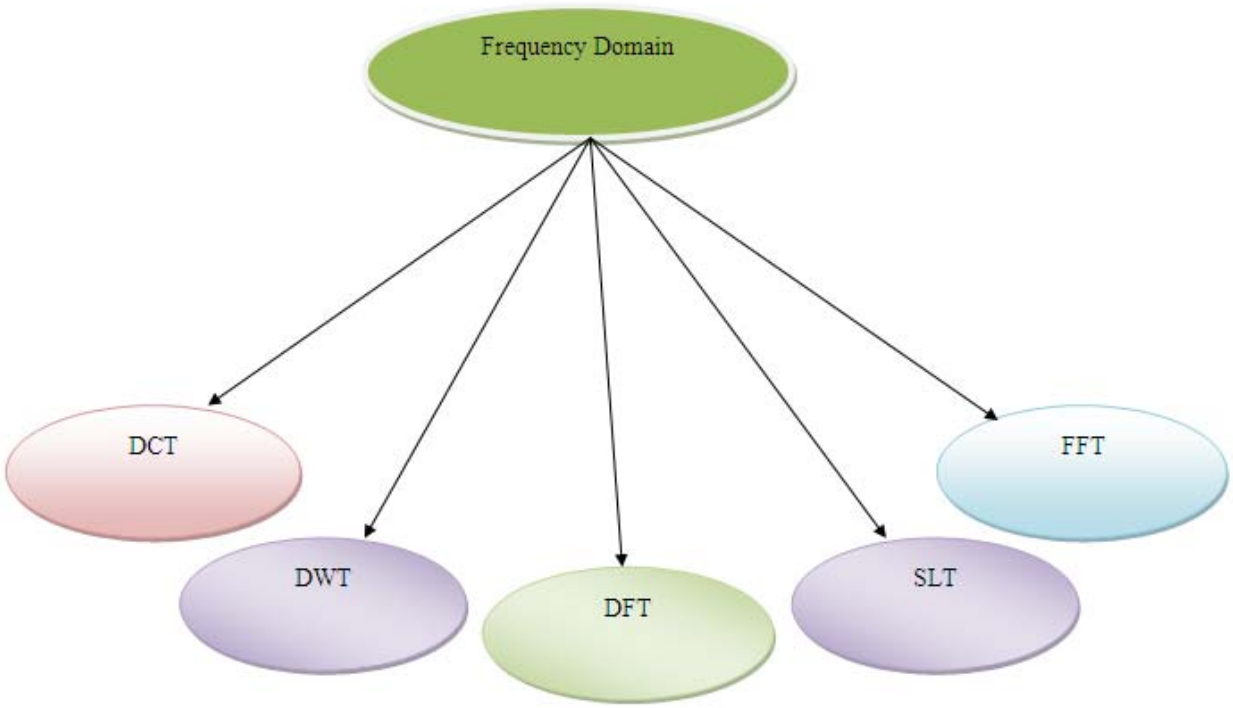

Figure3: Frequency Domain

- **Discrete cosine transforms (DCT):**
  A DCT [12] speaks to information as far as recurrence space instead of an abundancy space. Watermarking methods which depend on DCT are more hearty contrasted with spatial area strategies. These calculations are vigorous against computerized picture preparing operations like low pass separating, shine and difference alteration and so on. These are computationally more costly and are hard to execute. In the meantime they are frail against geometric assaults like turn, scaling, editing and so forth. DCT area watermarking can be arranged into Global DCT watermarking and Block based DCT water-stamping.

- **Discrete wavelet transforms(DWT):**
  This is a cutting edge strategy [9], broadly utilized as a part of computerized flag master cessing, picture pressure, watermarking and so on. The changes depend on little waves, called wavelet, of fluctuating recurrence and restricted term. This method utilizes wavelet channels to change the picture. The fundamental thought of DWT in picture process is to multi-separated deteriorate of picture into sub picture of various spatial space and autonomous frequenciesWatermarking techniques are proceeded by noise handling mechanisms acting as pre-processing mechanisms.

Various noises present within the images are described as under

- Impulse noise

The impulse noise [13] is caused by rise in temperature within the image. The pixels are phosphorous dots which will be exited with the rise in temperature. The exited pixels when comes to ground state emits energy in the form of light and distortion appears within the image. The image affected by the impulse noise has least clarity.

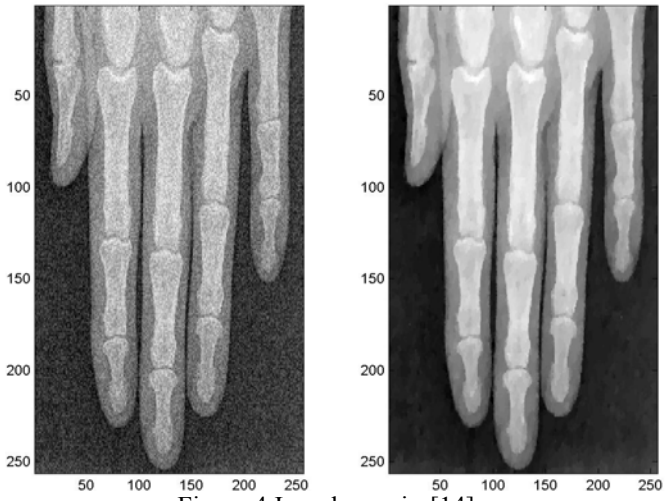

Figure 4:Impulse noise[14]

- Salt and pepper noise

This type of noise will reduce the clarity and spikes are introduced within the image. These spikes are introduced because of the intensity values which reach 0 02 maximum 255 level. The spikes within the image will cause spots within the image. The median filter is the mechanism which is used to tackle such noise.

Figure 5:Salt and pepper noise[15]

- Gaussian noise

It is a statistical noise whose probability distribution function is similar to original distribution. This will cause overlapping pixels and hence cause distortion within the image.

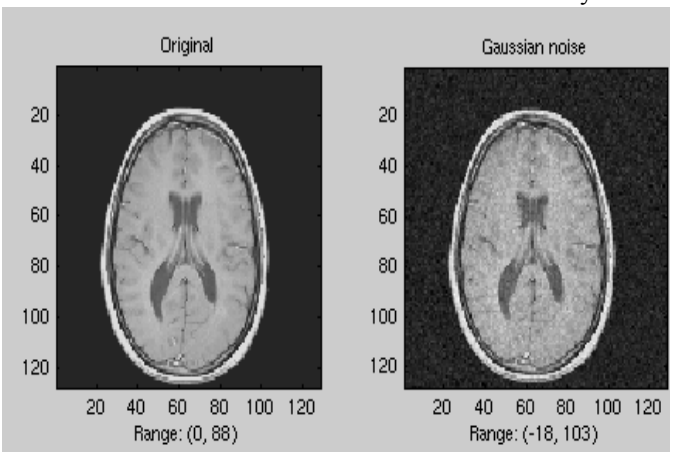

Figure 6: original image and image after Gaussiannoise[16]

In order to tackle such distortions median filter and homomorphic filters are present but these filters have to be used individually. This process is time consuming. So we propose universal filter which automatically detect and restore the image to its original state.

- Shot Noise

This type of noise takes place in the darker region of the image. This noise is caused due to the fluctuations present within the image. The fluctuations can cause the dark region within the image that will cause loss of information from the image.

Figure 7 shows shot noise[17]

- Quantization Error

The quantization error will be caused when the sampling is done. The sampling at the distinct interval of time is caused. The quantization error will distort the image and reduce the clarity within the image.

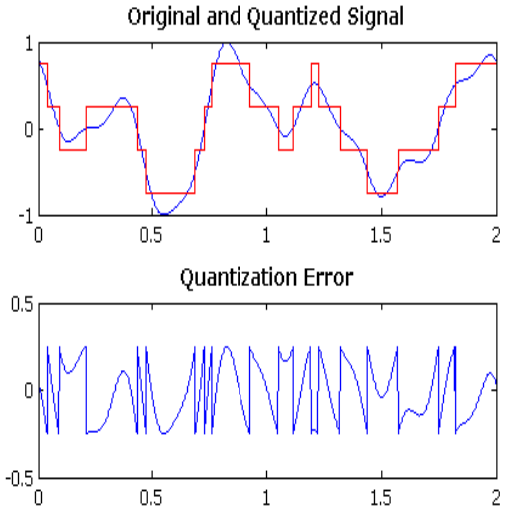

Figure 8 shows quantization error[18]

- Anisotropic Noise
  This type of noise is caused due to the manipulation of image. The distortion will cause contrast problem within the image.

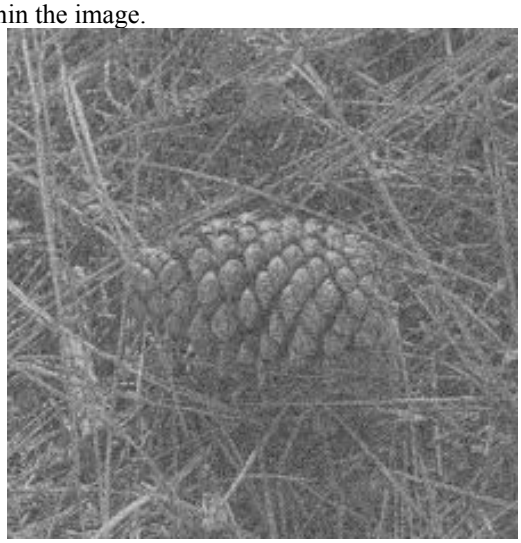

Figure9:showsanisotropicnoise[19]

In order to tackle the noise various filtering mechanisms are employed. Various filtering mechanisms are as described below

Filtering Mechanism

The filtering mechanism are used in order to enhance the performance of the image we will utilize the filtering mechanism. The filtering mechanism are described as follows

- Median Filter
  The median filter[20] is used in order to remove the salt and pepper noise from the image.

Figure10: shows median filter[20]

- Mean Filter
  The mean filter is also used in order to handle the noise. The noise is reduced by taking the mean of the neighboring pixel position. The mean filter generally operate in the spatial domain.

Figure 11 shows mean filter[20]

- Homomorphic Filter
  The Homomorphic filter [21] is used in order to enhance the capacity of the image by smoothening the image. The image attributes are enhanced by the use of filtering mechanism.

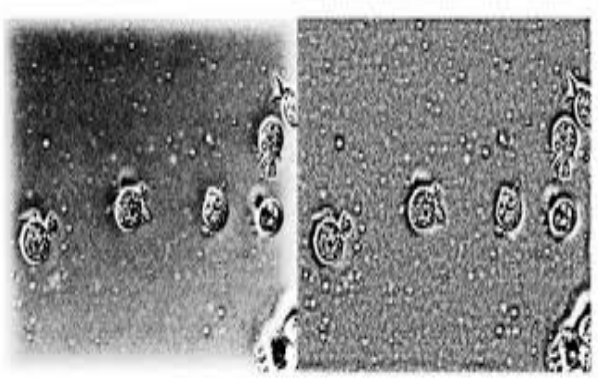

Figure12: shows homomorphicfilter[21]

The filtering mechanism is enforced due to problems present within the compression mechanisms. Next section described the earlier work to extract the best possible technique used for watermarking.

3. EXISTING WORK

The techniques associated with image encryption are described in this section.

Xu et al. 2011[22] haveproposed field of signal processing the technology of image watermark is very important. In this paper the knowledge of image watermark as well as the DCT/IDCT had been introduced. Encryption algorithm used for image size on which information of watermarking is based.To verify this watermarking algorithm by MATLAB the watermark's embedding and extraction had been performed on two images. The outcomes prove adaptive algorithm to be constructive.

Tiwari 2015[2] has proposed technology is improving in a great way with thischange in imaging aptitude. The straightforwardness with which advanced substance can be imitated and worked there is a solid prerequisite for a computerized patent gadget to be set up. It is required for the confirmation of the substance and also the proprietor and advanced watermarking is the solution to resolve this problem. We have several watermarking techniques have been introduced now. In this paper we survey the current schemes that have been developed with their effectiveness.

In Tun & Onn 2015[23] paper High efficiency video coding (HEVC) is the new video coding age of the ITU-T and ISO/IEC, which was first showed up in January 2013. Its primary leverage is that it lessens the bit rate by as much as 50 % when contrasted with H.264 despite the fact that visual quality is kept up. Keeping in mind the end goal to secure video substance by implanting inside a proficient video codec verification and copyright insurance approaches' have turned out to be one of the basic things. The primary goal of this paper is to overhaul late improvements in the territory of watermarking procedures for video coding plans and their pertinence to the new Standard HEVC. The results of this examination offer motivation to fulfill a higher introducing limit and higher weight execution for HEVC diverged from H.264/AVC especially, for low bitrate coding.

Han et al. 2015[4]have proposed paper works on medical information digitization storage and extraction process more convenient. In Medical picture data the security and copyright insurance is considered so important, with the goal that medicinal picture watermarking has been connected. This paper proposes a vigorous zero-watermarking calculation. This calculation depends on three-dimensional discrete wavelet change recurrence investigation highlights, which utilizes perceptual hashing procedure to extricate restorative volume information itself include vector keeping in mind the end goal to structure strong zero watermarking. The calculation accomplishes a mix of legendre turbulent neural system encryption and zero watermarking innovation, to enhance the medicinal volume information watermarking calculation security and heartiness. The reenactment comes about gives the viability of the calculation.

Wang et al. 2015[24]have proposed paper for data transfer in terms of collaborating images which can be LSB or MSB watermarking, adigital watermarking based copyright protection method is proposed for wireless sensor networks data security. This method of manipulating both LSB and MSRB bits of the data field data, the embedding capacity can be expanded. In addition to above technology, two-dimensional code based on the test results are generated, and facilitates the user's copyright authentication.

Mundher et al. 2014[25] Proposed paper presents digital images watermarking to provide ownership and true authentication. To secure the images, audio and videos, Firstly watermark W is converted into a sequence of bits and in order to encrypt the watermark, sequence of size R is selected randomly. Secondly, a pseudo random number is generated to calculate pixels for selection key generation. Finally, 2-level discrete slanted transform (DST) on the host image is applied to divide it into Red, Green and Blue channels. The results exhibit robustness against the existing state of the art. Further, In the absence of the original images proposed approach effectively extract watermark.

Cohen n.d.[26]has proposed paper uses watermarking scheme in which a mark is dropped into group of instruction forming a program for watermarking. In considered paper different issues of watermarking cryptographic projects, for example, pseudorandom work (PRF) assessment, unscrambling, and marking are examined. In our proposed paper, watermarking plans utilized as an open key, implying that we utilize a mystery checking key to install stamps in programs, and an open location key that enables anybody to distinguish stamps in programs. Our security idea of watermark non-removability considers arbitrary antagonistic systems to alter the stamped program, as opposed to the earlier works

Badshah et al. 2015[27] have proposed paper the innovation of watermarking assumes a critical part in a large portion of the businesses for giving security to their own and additionally enlisted or rented information. In proposed paper investigation of Spatial and Fractal watermarking calculation is utilized to enhance the protection in information pressure. In the Spatial domain method, there is no costly transforms needed to be computed for watermark embedding. The luminance values will be manipulated directly. For the implementation of watermarking concept, we have used minimum nine coordinate positions. The watermarking algorithms that we have used are Bruyn algorithm and Langelaar algorithm. Result is given in terms of graph for better understanding. While dealing with digital image processing image is represented using graphical user interface allowing better interactivity.

Gupta 2012[28] has proposed paper for copyright protection of multimedia data, Digital watermarking is one of the best solution. It is better than Digital Signatures and other methods because it does not increase overhead. To shroud data, for instance a number or content, in advanced media, for example, pictures, video or sound computerized watermarking is utilized. The implanting happens by controlling the substance of the computerized information, which implies the data isn't installed in the edge around the information. In this paper cryptography based Blind picture watermarking procedure displayed that can implant more number of watermark bits in the dark scale cover picture without influencing the intangibility and increment the security of watermarks.

Furon 2005[29]hasProposed paper of Digital watermarking for the improvement and robustness in multimedia. This paper presents an overview of secure watermarking technique. For each context, a threat analysis is purposed. This study allows us to illustrate all the certainties the

community has on the subject, browsing all key papers. In future vague facts, intuitions will be discussed.

Hari & Sarvanan 2014[30]talked about a review on computerized watermarking process, applications, idea and its commitments in different fields is presented. Computerized watermarking conceals the critical from unlawful duplication and dispersion of media information. Watermarking is one of the imperative application in the picture handling .Watermarking is the way toward embedding the watermarked message in a host record in some mixed media arrangement to shield the data from the unapproved get to.The photo watermarking systems may segment on the introduce of space like spatial range or change territory or on the start of wavelets. The copyright assurance, limit, security, vigor and so forth are a portion of the critical components that are considered while the watermarking framework is outlined.

Kekre 2015[31] discussed about a half and half watermarking method utilizing Singular esteem Decomposition with orthogonal changes like DCT, Haar, Walsh, Real Fourier Transform and Kekre change is proposed in this paper. Afterward, SVD is joined with wavelet changes produced from these orthogonal transforms. Singular values of watermark are embedded in middle frequency band of column/row transform of host image.Before installing, Singular esteems are scaled with reasonable scaling factor and are arranged. Segment/push change decreases the computational many-sided quality to half and properties of solitary esteem disintegration and changes add to heartiness. Conduct of proposed technique is assessed against different assaults like pressure, trimming, resizing, and clamor expansion. For larger part of assaults wavelet changes end up being more powerful than comparing orthogonal change from which it is produced.

Gupta et al. 2015[32] discussed about the development of innovation has made a few straightforward approaches to control the first substance. This has brought the worry for security of the substance which is effectively accessible in open system. Electronic watermarking is the most proper response for the characterized issue. Advanced watermarking is the specialty of embedding the logo into sight and sound question have confirmation of possession at whatever point it is required. The proposed calculation is valuable in approved dissemination and possession confirmation. The calculation utilizes the concept of AC forecast utilizing DCT to implant the watermark in the picture. The calculation has phenomenal heartiness against every one of the assaults and beats the comparative work with commendable performance regarding Normalized Correlation (NC), Peak Signal to Noise Ratio (PSNR) and Tamper Assessment Function (TAF).

Mane & Chiddarwar 2013[33] have proposed the protection and illegal redistribution of digital media has become an important issue in the digital era. This is due to the popularity and accessibility of the Internet now a days by people. This results in recording, editing and replication of multimedia contents.To protect information from illegitimate modifications we can use digital watermarking. Computerized watermarking system is the way toward installing noise-tolerant signal, for example, sound or picture information in the bearer signal. This system gives a strong answer for the issue of protected innovation rights for online substance.This paper reviews different aspects and techniques of digital watermarking for protecting digital contents.

Awodele & Ogbonna 2015[34] have proposed paper on Cyber security which is for the most part an expansion of the conventional data innovation (IT) security that is gone for ensuring frameworks, applications and information that presented to an assortment of types of assault through the web, going from information burglary and secret activities to defilement of information and disavowal of administration assaults.There is a requirement for an increase in digital security examine because of misfortunes from undermine being experienced by countries, organizations and people from different cybercrime assaults. This paper investigates the applications advanced watermarking to the procedure of assurance in the internet called digital watermarking especially concentrating on burglary of data (personality and charge card theft).The technique of the examination is through writing inquiry and contextual analysis. Whatever is left of the paper shows a concise outline of the advanced watermarking and issues in digital security.

Chitla & M 2014[35]have talked about across the board utilization of the Internet in the current past has demonstrated its effect in upgrading the development in different fields, for example, in instruction, keeping money, business, medication, military applications and some more. In the ebb and flow e-wellbeing applications where pictures are put away, recovered and transmitted over the web, advanced watermarking assumes a fundamental part in validating the restorative pictures, content confirmation, ensuring the photo quality and improving the data security. The present paper is a discourse on watermarking systems that are useful in confirming the medicinal pictures with a study of most recent research in the zone. This paper likewise thinks about the reproduction consequences of watermarking and recuperation of watermark on a few assaults on various therapeutic pictures.

Dhull 2013[36] discussed in this paper that everyday large amount of data is embedded on digital media and spread over the internet. This data can easily be replaced without error. Advanced watermarking is the most imperative innovation in this day and age, to anticipate unlawful replicating of information. Computerized watermarking can be connected to sound, video, content or pictures.

In (Science & Studies 2015)[37]paper in order to protect copyrighted material, particularly advanced pictures, analysts have concentrated on the procedure named as computerized watermarking. In the proposed paper, the premise of hued picture watermarking is talked about taken after by a fundamental system for watermarking shaded pictures have been proposed in changed area.

Tomar 2015[38] has proposed that Digital watermarking technique is becoming more important in this developing society of internet.Computerized watermarking is utilized to secure the data against the illicit circulation as pictures, recordings and sounds. Computerized watermark strategies are utilized as a part of different territories, for example, copyright assurance, communicate monitoring and proprietor recognizable proof. Computerized picture watermarking strategy is the way toward implanting watermark as picture that contain the extraordinary data and then it distinguish and extricate that unique data. The vigor, copyright insurance, loyalty, limit and some more are

fundamental necessities of watermarking plans so they can handle a few sorts of assaults. This paper surveys distinctive perspectives and procedures of computerized picture watermarking and diverse Walsh Coding Algorithm.

Yan et al. 2015[39] have proposed that the autoregressive (AR) display is broadly utilized as a part of demonstrating picture, discourse and EEG signals. Using this model as the model for the host flag, we have figured a watermarking estimation which is pleasant with the power go condition. This is expert by introducing the quantization watermark in the extra flag of the AR illustrate, both for dither modification (DM) watermarking and spread-change dither control (STDM) watermarking. This paper similarly analyzes the unraveling execution. A logical outcome is gotten, which portrays the connection between the deciphering blunder rate and the flag to commotion proportion, show parameters and the length of the vector. This examination result is checked through numerical investigations. Utilizing this examination result, a planner of the watermarking framework can decide the outline parameters in view of the particular of the given framework execution record.

4. COMPARISON OF VARIOUS IMAGE WATERMARKING TECHNQIUES

Table 1: Comparison of Image Encryption Techniques

Title And Reference	Parameters	Techniques	Merit	Demerit
(Islam et al. 2017)[40] An Improved Image Steganography Technique based on MSB using Bit Differencing	MSE PSNR	IMAGE STEGNOGRAPHY	MSB steganography is used for image security. MSE and PSNR is improved	MSB steganography may lead to distortion within the image. Entropy can be further maximised
(Gonge 2016)[41] An Integration of SVD Digital Image Watermarking with AES Technique for Copyright Protection and Security of Bank Cheque Image	RMSE	SVD	Singular valued decomposition provides least complexity in terms of gray scale images hence classification is better. RMSE is low	Coloured images cannot be tackled. PSNR can be further improved
(Sheth &Nath 2016)[42] Secured Digital Image Watermarking with Discrete Cosine Transform and Discrete Wavelet Transform method	Compression Ratio PSNR	DCT AND DWT	Modularity is enhanced due to the application of DWT. Compression preserve space and PSNR ensure better contrast	Complexity of mathematical calculations is high due to DCT MSE can be further reduced
(Mahule 2015)[43] Analysis of Image Security Techniques using Digital Image Watermarking in Spatial Domain	MSE	Spatial Domain based on LSB- Based, Statistical-Based, Feature-Based and Block-Based.	Analysis of various techniques for security enhancement is presented which can be used for further enhancement in image security. MSE hence is low	No parameter wise description is presented. PSNR can be further improved
(Mundher et al. 2014)[25] Digital Watermarking for Images Security using Discrete Slantlet Transform	MSE PSNR	DST	Effective extraction of features for security enhancement hence MSE is low and PSNR is high	Complex due to heavy mathematical calculations. Entropy can be further improved
(Science & No n.d.)[44] A Digital Image Watermarking Algorithm Based on Discrete Wavelet Transform and Discrete Cosine Transform	MSE PSNR	DCT DWT	Application of DCT is presented for enhancement of security in terms of data hiding in images. PSNR is high and MSE is low	Time complexity of overall operation is high due to limited modularity. Security keys can be further made strong
(Gupta & Singh	Compression	CRYPTOGR	Enhanced security is	Complexity of

2014)[45]New Proposed Practice for Secure Image Combing Cryptography Stenography and Watermarking based on Various Parameters	Ratio MSE PSNR	APHY, STEGNOGRAPHY AND WATERMARKING	achieved through the application of hybridization. MSE is low and PSNR is high. Space preservation is present	operation is enhanced. Entropy can be further optimised
(Ramani et al. n.d.)[46]Protecting Digital Images Using DTCWT-DCT	Compression Ratio	DTCWT-DCT	Hybridization is done to reduce time complexity. Image watermarking security is enhanced using proposed technique	Space complexity is high and nothing is suggested to reduce this complexity
(Xu et al. 2011)[22]Research on Image Watermarking Algorithm based on DCT	Compression Ratio	DCT	Watermarking security is enhanced using DCT. Efficient compression for space preservation	Complexity in terms of space and time is high. MSE is high and PSNR is low which can be improved
(Bhatnagar et al. 2010)[47] Biometric Template Security based on Watermarking	Entropy	BIOMETRIC SECURITY	Biometric security is enhanced through watermarking. Entropy is high	Hybridization of multiple approaches is missing PSNR and MSE can be further improved

Table 2: Comparison of Optimized parameters proved within the analyzed papers.

Title And Reference	Parameters	Optimised Parameter
(Islam et al. 2017)[40] An Improved Image Steganography Technique based on MSB using Bit Differencing	MSE PSNR	MSE is optimised but PSNR is reduced
(Gonge 2016)[41] An Integration of SVD Digital Image Watermarking with AES Technique for Copyright Protection and Security of Bank Cheque Image	RMSE	RMSE is optimised
(Sheth & Nath 2016)[42] Secured Digital Image Watermarking with Discrete Cosine Transform and Discrete Wavelet Transform method	Compression Ratio PSNR	Compression reduced the size of the image but PSNR can be further optimised
(Mahule 2015)[43]Analysis of Image Security Techniques using Digital Image Watermarking in Spatial Domain	MSE	MSE is reduced considerably,

5. RESEARCH GAPS

The existing techniques used mechanism to secure the data transmission. The problem however persist since during decoding of information some part of information may be lost. The clarity of information may also be lost hence PSNR(Peak signal to noise ratio) is considerably reduced. Also MSE(Mean Square Error) is high. These parameters required to be enhanced in future.

6. CONCLUSION

The real challenges of today's era are sending information safely on Internet. Various techniques such as encryption, steganography etc.havebeen evolved over the years the efficiency and energy consumption associated with these techniques still require improvement .Watermarking security is one of the alternatives for enhancing the security process. The watermarking security utilizes two consecutive images and merges them together, after merging

images transferred towards the destination. In case of corruption images distorted and techniques such as SVD, DWT can be used to analysis such images. MSE and accuracy associated with SVD, DWT is not optimum.In future slant let transformation along with SVD can be used in order to improve MSE and accuracy.

REFERENCES

[1] Aparna J R & Ayyappan, S., 2014. Comparison of digital watermarking techniques. 2014 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC), pp.87–92.

[2] Tiwari, G., 2015. A Review on Robust Watermarking with its Applications and Comparative Analysis. , 8(6), pp.85–90.

[3] Pramkeaw, P., Ganokratanaa, T. & Phatchuay, S., 2016. Integration of Watermarking and QR Code for Authentication of Data Center. 2016 12th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), pp.669–672. Available at: http://ieeexplore.ieee.org/document/7907538/.

[4] Han, B., Cai, L. & Li, W., 2015. Zero-watermarking Algorithm for Medical Volume Data Based on Legendre Chaotic Neural Network and Perceptual Hashing. , 8(1), pp.201–212.

[5] Bathinda, T., 2016. Invisible Video Multiple Watermarking Using Optimized Techniques.

[6] Dabas, P., 2013. A study on spatial and transform domain watermarking techniques. International journal of computer applications, 71(14), pp.38–41.

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

[8] Tyagi, S. & Singh, H.V., 2016. Digital Watermarking Techniques for Security Applications.

[9] Yadav, U. et al., 2014. Different Watermarking Techniques & its Applications: A Review. International Journal of Scientific & Engineering Research, 5(4), pp.1288–1294.

[10] Fang, L. & Dobson, S., 2014. Data Collection with In-network Fault Detection Based on Spatial Correlation. Cloud and Autonomic Computing (ICCAC), 2014 International Conference on, pp.56–65.

[11] Beiji, Z. & Abdullah, M.Y., 2011. Information Security Technique in Frequency Domain. , 5(December), pp.279–289.

[12] Kaur, A. & Kaur, J., 2012. Comparision of Dct and Dwt of Image Compression Techniques. , 1(4), pp.49–52.

[13] Kandpal, A. & Ramola, V., 2015. Global Image Segmentation Process for Noise Reduction by Using Median Filter. , 3(3), pp.201–206.

[14] Leavline, E.J., Antony, D.A. & Singh, G., 2013. Salt and Pepper Noise Detection and Removal in Gray Scale Images : An Experimental Analysis. , 6(5), pp.343–352.

[15] Pilevar, A.H. et al., 2015. A new filter to remove salt and pepper noise in color images. Signal, Image and Video Processing, 9(4), pp.779–786.

[16] Ma, Y. et al., 2007. A Novel Algorithm of Image Gaussian Noise Filtering based on PCNN Time Matrix. In 2007 IEEE International Conference on Signal Processing and Communications. IEEE, pp. 1499–1502. Available at: http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=4728615 [Accessed June 2, 2016].

[17] Djidjou, T.K. et al., 2014. Observation of Shot Noise in Phosphorescent Organic Light-Emitting Diodes. , 61(9), pp.3252–3257.

[18] Kasat, N.R. & Thepade, S.D., 2016. Novel Content Based Image Classification Method Using LBG Vector Quantization Method with Bayes and Lazy Family Data Mining Classifiers.

[19] Khalvati, F., 2008. Computational Redundancy in Image Processing. Image (Rochester, N.Y.), (November).

[20] Kumari, A., Thomas, P.J. & Sahoo, S.K., 2015. Single image fog removal using gamma transformation and median filtering. 11th IEEE India Conference: Emerging Trends and Innovation in Technology, INDICON 2014.

[21] Raju, K.M.S., Nasir, M.S. & Devi, T.M., 2013. Filtering Techniques to reduce Speckle Noise and Image Quality Enhancement methods on Satellite Images. , 15(4), pp.10–15.

[22] Xu, Z.J., Wang, Z.Z. & Lu, Q., 2011. Research on Image Watermarking Algorithm based on DCT. , 10, pp.1129–1135.

[23] Tun, U. & Onn, H., 2015. RECENT METHODS AND TECHNIQUES IN VIDEO WATERMARKING AND THEIR APPLICABILITY TO THE. , 74(1).

[24] Wang, B. et al., 2015. A Copyright Protection Method for Wireless Sensor Networks Based on Digital Watermarking. , 8(6), pp.257–268.

[25] Mundher, M. et al., 2014. Digital Watermarking for Images Security using Discrete Slantlet Transform. , 2830(6), pp.2823–2830.

[26] Cohen, A., Watermarking Cryptographic Capabilities ∗.

[27] Badshah, G. et al., 2015. Importance of Watermark Lossless Compression in Digital Medical Image Watermarking. , 4(3), pp.75–79.

[28] Gupta, P., 2012. Cryptography based digital image watermarking algorithm to increase security of watermark data. , 3(9), pp.1–4.

[29] Furon, T., 2005. A Survey of Watermarking Security. , pp.201–215.

[30] Hari, B. & Sarvanan, T., 2014. A survey on Digital Image Watermarking. , 1(4), pp.49–53.

[31] Kekre, H.B., 2015. Performance Comparison of Watermarking Using SVD with Orthogonal Transforms and Their Wavelet Transforms. , (March), pp.1–18.

[32] Gupta, G., Joshi, A.M. & Sharma, K., 2015. AN EFFICIENT ROBUST IMAGE WATERMARKING BASED ON AC PREDICTION TECHNIQUE USING DCT TECHNIQUE Watermarked image. , 9102(August), pp.1055–1059.

[33] Mane, G. V & Chiddarwar, G.G., 2013. Review Paper on Video Watermarking Techniques. , 3(4), pp.1–5.

[34] Awodele, O. & Ogbonna, A.C., 2015. Applications of Digital Watermarking to Cyber Security (Cyber Watermarking). , pp.1–11.

[35] Chitla, A. & M, C.M., 2014. Authenticating Medical Images with Lossless Digital Watermarking. , (April), pp.291–296.

[36] Dhull, S., 2013. Digital watermarking. , 3(4), pp.280–283.

[37] Science, C. & Studies, M., 2015. Colored Image Watermarking : A Basis. , 7782, pp.148–152.

[38] Tomar, K., 2015. International Journal of Advanced Research in Computer Science and Software Engineering A Review Paper of Different Techniques on Digital Image Watermarking Scheme for Robustness. , 5(2), pp.900–904.

[39] Yan, B., Wang, Y. & Song, L., 2015. Power Spectrum Compliant QIM Watermarking for Autoregressive Host Signals. , 6(5), pp.882–888.

[40] Islam, A.U. et al., 2017. An improved image steganography technique based on MSB using bit differencing. 2016 6th International Conference on Innovative Computing Technology, INTECH 2016, pp.265–269.

[41] Gonge, S.S., 2016. An Integration of SVD Digital Image Watermarking with AES Technique for Copyright Protection and Security of Bank Cheque Image. , pp.769–778.

[42] Sheth, R.K. & Nath, V. V., 2016. Secured digital image watermarking with discrete cosine transform and discrete wavelet transform method. 2016 International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Spring), pp.1–5. Available at: http://ieeexplore.ieee.org/document/7578861/.

[43] Mahule, R. V, 2015. Analysis of Image Security Techniques using Digital Image Watermarking in Spatial Domain. , (Nckite), pp.19–26.

[44] Science, I. & No, W., A Digital Image Watermarking Algorithm Based on Discrete Wavelet Transform and Discrete Cosine Transform Yang Qianli. , pp.1102–1105.

[45] Gupta, R. & Singh, T.P., 2014. New proposed practice for secure image combing cryptography stegnography and watermarking based on various parameters. Proceedings of 2014 International Conference on Contemporary Computing and Informatics, IC3I 2014, pp.475–479.

Procedia Computer Science, 79, pp.483–489.

[46] Ramani, K., Prasad, E. V & Varadarajan, S., Protecting Digital Images Using DTCWT-DCT. , pp.36–44.

[47] Bhatnagar, G., Wu, Q.M.J. & Raman, B., 2010. Biometric Template Security based on Watermarking. Procedia Computer Science, 2, pp.227–235. Available at: http://dx.doi.org/10.1016/j.procs.2010.11.029.