International Journal of Advance Research in Science and Engineering
Volume No.06, Special Issue No.(03), December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

Study of security enhancement strategies in digital image processing

Neha Mahant[1] , Assist. Prof. Sharanjit Singh[2]

[1,2]Computer Science and Engg. Department , Regional campus ,GNDU,Gurdaspur(India)

ABSTRACT

The accessibility of internet now days are more by people that give rise to the problem of protection of digital media and their distribution over the internet . To protect digital media from any unauthorized access digital watermarking has to be utilized. It is a way through which a watermark in the form of image has been embedded and it contains special information. This paper reviews various techniques of digital watermarking, watermarking applications. Also some recent research in the field of watermarking techniques for text documents also reviewed.

Keywords*: *Frequency watermarking technique, Spatial watermarking technique,Types of watermarking, Watermarking.

I.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 they both conceal messages inside a digital signal. The fundamental distinction between the two is: Watermarking tries to hide a message that is identified with real substance of the digital flag. Yet Steganography has no contact to the message. It is utilized similarly as a cover to shroud a message. 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 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 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.

II.LITERATURE SURVEY

The techniques associated with image encryption are described in this section. [1] Proposed 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 had been introduced in which the watermarking information was based on the size of the image. To verify this watermarking algorithm by MATLAB the watermark’s embedding and extraction had been performed on two images. The result shows that the adaptive algorithm is very effective. [2] Proposed technology is improving in a great way with this improvement in imaging skill. The ease with which digital content can be imitated and operated there is a strong requirement for a digital patent device to be put in place. It is required for the authentication of the content as well as the owner and digital 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 [3] paper High efficiency video coding (HEVC) is the new video coding generation of the ITU-T and ISO/IEC, which was first appeared in January 2013. Its main advantage is that it reduces the bit rate by as much as 50 % when compared to H.264 even though visual quality is maintained. In order to protect video contents by embedding within an efficient video codec authentication and copyright protection methodologies have become one of the essential items. The main objective of this paper is to revise recent developments in the area of watermarking techniques for video coding schemes and their applicability to the new Standard HEVC. The results of this study provide motivation to achieve a higher embedding capacity and higher compression performance for HEVC compared to H.264/AVC especially, for low bitrate coding.

[4] Proposed paper works on medical information digitization storage and extraction process more convenient. In Medical image information the security and copyright protection is taken so seriously, so that medical image

watermarking has been applied. This paper proposes a robust zero-watermarking algorithm. This algorithm is based on three-dimensional discrete wavelet transform frequency analysis features, which uses perceptual hashing technique to extract medical volume data itself feature vector in order to structure robust zero watermarking. The algorithm achieves a combination of legendre chaotic neural network encryption and zero watermarking technology, to improve the medical volume data watermarking algorithm security and robustness. The simulation results gives the effectiveness of the algorithm[5].

In [6]proposed paper wireless sensor networks are group of sensor nodes in the monitored area. In these networks, data security from sensors has been threatened. In this paper, a digital 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.

[7] 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.

[8] Proposed paper uses watermarking scheme in which a mark is dropped into a program while preserving its functionality. Nobody can remove the mark without damaging the functionality of the program. In this paper various problems of watermarking cryptographic programs such as pseudorandom function (PRF) evaluation, decryption, and signing are studied. In our proposed paper, watermarking schemes used as a public key, meaning that we use a secret marking key to embed marks in programs, and a public detection key that allows anyone to detect marks in programs. Our security notion of watermark non-removability considers arbitrary adversarial strategies to modify the marked program, in contrast to the prior works

In [9] proposed paper the technology of watermarking plays a pivotal role in most of the industries for providing security to their own as well as hired or leased data. In proposed paper study of Spatial and Fractal watermarking algorithm is used to improve the resistance in data compression. 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. In graph, we have plotted X axis as peak signal to noise ratio (PSNR) and y axis as Correlation with original watermark. The threshold value ά is set to 5. If the result is smaller than the threshold value then it is feasible, otherwise not

In [10] 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 hide information, for example a number or text, in digital media, such as images, video or audio digital watermarking is used. The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data. In this paper cryptography based Blind image watermarking technique presented that can embed more number of watermark bits in the gray scale cover image without affecting the imperceptibility and increase the security of watermarks.

[11] Proposed paper discussed 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 dicussed.

[12] In this paper a survey on digital watermarking process, applications, concept and its contributions in various fields is introduced. Digital watermarking helps to hide the crucial from illegal duplication and distribution of multimedia data. Watermarking is one of the important application in the image processing .Watermarking is the process of inserting the watermarked message in a host document in some multimedia format to protect the information from the unauthorized access. The image watermarking techniques may divide on the basis of domain like spatial domain or transform domain or on the basis of wavelets. The copyright protection, capacity, security, robustness etc are some of the important factors that are taken in account while the watermarking system is designed.

[13] A hybrid watermarking technique using Singular value Decomposition with orthogonal transforms like DCT, Haar, Walsh, Real Fourier Transform and Kekre transform is proposed in this paper. Later, SVD is combined with wavelet transforms generated from these orthogonal transforms. Singular values of watermark are embedded in middle frequency band of column/row transform of host image. Before embedding, Singular values are scaled with suitable scaling factor and are sorted. Column/row transform reduces the computational complexity to half and properties of singular value decomposition and transforms add to robustness. Behaviour of proposed method is evaluated against various attacks like compression, cropping, resizing, and noise addition. For majority of attacks wavelet transforms prove to be more robust than corresponding orthogonal transform from which it is generated.

[14] The expansion of technology has made several simple ways to manipulate the original content. This has brought the concern for security of the content which is easily available in open network. Digital watermarking is the most suitable solution for the defined issue. Digital watermarking is the art of inserting the logo into

multimedia object to have proof of ownership whenever it is required. The proposed algorithm is useful in authorized distribution and ownership verification. The algorithm uses the concept of AC prediction using DCT to embed the watermark in the image. The algorithm has excellent robustness against all the attacks and outperforms the similar work with admirable performance in terms of Normalized Correlation (NC), Peak Signal to Noise Ratio (PSNR) and Tamper Assessment Function (TAF).

[15] 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. Digital watermarking can be used to protect digital information against illegal manipulations and distributions. Digital watermarking technique is the process of embedding noise-tolerant signal such as audio or image data in the carrier signal. This technique provides a robust solution to the problem of intellectual property rights for online contents. This paper reviews different aspects and techniques of digital watermarking for protecting digital contents.

[16] Cyber security is generally an extension of the traditional information technology (IT) security that is aimed at protecting systems, applications and data that exposed to a variety of forms of attack via the internet, ranging from data theft and espionage to corruption of data and denial of service attacks. There is a need for an increase in cyber security research due to losses from sabotage being experienced by nations, businesses and individuals from various cybercrime attacks. This paper takes a look at the applications digital watermarking to the process of protection in cyber space called cyber watermarking particularly focusing on theft of information (identity & credit card theft).The methodology of the research is through literature search and case study. The rest of the paper presents a brief overview of the digital watermarking and issues in cyber security

[17] Wide spread of the Internet in the recent past has shown its impact in enhancing the growth in various fields such as in education, banking, commerce, medicine, military applications and many more. In the current e-health applications where images are stored, retrieved and transmitted over the internet, digital watermarking plays a vital role in authenticating the medical images, content verification, preserving the image quality and enhan cing the data security. The present paper is a detailed discussion on watermarking techniques that are helpful in authenticating the medical images with a survey of latest research in the area. This paper also studies the simulation results of watermarking and recovery of watermark on several attacks on different medical images.

[18] Everyday large amount of data is embedded on digital media and spread over the internet. This data can easily be replaced without error. Digital watermarking is the most important technology in today’s world, to prevent illegal copying of data. Digital watermarking can be applied to audio, video, text or images.

[19] In order to protect copyrighted material, especially digital images, researchers have focused on the technique termed as digital watermarking. In the proposed paper, the basis of colored image watermarking is

discussed followed by a basic technique for watermarking colored images have been proposed in transformed domain.

[20] Digital watermarking technique is becoming more important in this developing society of internet. Digital watermarking is used to protect the information against the illegal distribution in the form of images, videos and audios. Digital watermark techniques are used in various areas such as copyright protection, broadcast monitoring and owner identification. Digital image watermarking technique is the process of embedding watermark in the form of image that contain the special information and then it detect and extract that special information. The robustness, copyright protection, fidelity, capacity and some more are essential requirements of watermarking schemes so that they can handle several types of attacks. This paper reviews different aspects and techniques of digital image watermarking and different Walsh Coding Algorithm.

[21] The autoregressive (AR) model is widely used in modeling image, speech and EEG signals. Using this model as the model for the host signal, we have devised a watermarking algorithm which is compliant with the power spectrum condition. This is achieved by embedding the quantization watermark in the residual signal of the AR model, both for dither modulation (DM) watermarking and spread-transform dither modulation (STDM) watermarking. This paper also analyzes the decoding performance. An analytic result is obtained, which describes the relationship between the decoding error rate and the signal to noise ratio, model parameters and the length of the vector. This analysis result is verified through numerical experiments. Using this analysis result, a designer of the watermarking system can determine the design parameters based on the specification of the given system performance index.

III.COMPARISON OF VARIOUS IMAGE WATERMARKING TECHNQIUES

TITLE AND REFERENCE	JOURNAL/CONFERENCE	TECHNIQUE	MERIT	DEMERIT
[7] Digital Watermarking for Images Security using Discrete Slantlet Transform	NSP	DST	Effective extraction of features for security enhancement	Complex due to heavy mathematical calculations
[22] Analysis of Image Security	IJCA	Spatial Domain based on LSB-Based, Statistical-	Analysis of various techniques for	No parameter wise description is

Techniques using Digital Image Watermarking in Spatial Domain		Based, Feature-Based and Block-Based	security enhancement is presented which can be used for further enhancement in image security	presented
[23] A Digital Image Watermarking Algorithm Based on Discrete Wavelet Transform and Discrete Cosine Transform	IEEE Conference	DCT	Application of DCT is presented for enhancement of security in terms of data hiding in images	Time complexity of overall operation is high due to limited modularity
[24] An Integration of SVD Digital Image Watermarking with AES Technique for Copyright Protection and Security of Bank Cheque Image	IEEE	SVD	Singular valued decomposition provides least complexity in terms of gray scale images hence classification is better	Coloured images cannot be tackled
[1] Research	SCIENCE DIRECT	DCT	Watermarking	Complexity

on Image Watermarking Algorithm based on DCT			security is enhanced using DCT	in terms of space and time is high
[25] Protecting Digital Images Using DTCWT-DCT	IEEE	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
[26] Secured Digital Image Watermarking with Discrete Cosine Transform and Discrete Wavelet Transform method	IEEE	DCT AND DWT	Modularity is enhanced due to the application of DWT	Complexity of mathematical calculations is high due to DCT
[27] Biometric Template Security based on Watermarking	SCIENCE DIRECT	BIOMETRIC SECURITY	Biometric security is enhanced through watermarking	Hybridization of multiple approaches is missing
[28] An Improved	IEEE	IMAGE STEGNOGRAPHY	MSB Stegnography	MSB Stegnograph

Image Steganography Technique based on MSB using Bit Differencing			is used for image security	y may lead to distortion within the image
[29] New Proposed Practice for Secure Image Combing Cryptography Stegnography and Watermarking based on Various Parameters	IEEE	CRYPTOGRAPHY , STEGNOGRAPHY AND WATERMARKIN G	Enhanced security is achieved through the application of hybridization	Complexity of operation is enhanced

Table 1: Comparison of Image Encryption Techniques

IV.CONCLUSION

The security within transfer of information is critical. Various techniques such s encryption, steganography etc has been 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.

So in future slant let transformation along with SVD can be used in order to improve MSE and accuracy.

REFERENCES

[1] Z. J. Xu, Z. Z. Wang, and Q. Lu, "Research on Image Watermarking Algorithm based on DCT," vol. 10, pp. 1129–1135, 2011.

[2] G. Tiwari, "A Review on Robust Watermarking with its Applications and Comparative Analysis," vol. 8, no. 6, pp. 85–90, 2015.

[3] U. Tun and H. Onn, "RECENT METHODS AND TECHNIQUES IN VIDEO WATERMARKING AND THEIR APPLICABILITY TO THE," vol. 74, no. 1, 2015.

[4] B. Han, L. Cai, and W. Li, "Zero-watermarking Algorithm for Medical Volume Data Based on Legendre Chaotic Neural Network and Perceptual Hashing," vol. 8, no. 1, pp. 201–212, 2015.

[5] G. Badshah, S. Liew, J. M. Zain, S. I. Hisham, and A. Zehra, "Importance of Watermark Lossless Compression in Digital Medical Image Watermarking," vol. 4, no. 3, pp. 75–79, 2015.

[6] B. Wang, J. Su, Y. Zhang, B. Wang, and J. Shen, "A Copyright Protection Method for Wireless Sensor Networks Based on Digital Watermarking," vol. 8, no. 6, pp. 257–268, 2015.

[7] M. Mundher, D. Muhamad, A. Rehman, T. Saba, and F. Kausar, "Digital Watermarking for Images Security using Discrete Slantlet Transform," vol. 2830, no. 6, pp. 2823–2830, 2014.

[8] A. Cohen, "Watermarking Cryptographic Capabilities ∗."

[9] S. T. Kannan and S. A. Senthil, "A Frame Work for Various Watermarking Algorithms," vol. 4, no. 1, pp. 21–28, 2015.

[10] P. Gupta, "Cryptography based digital image watermarking algorithm to increase security of watermark data," vol. 3, no. 9, pp. 1–4, 2012.

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

[12] B. Hari and T. Sarvanan, "A survey on Digital Image Watermarking," vol. 1, no. 4, pp. 49–53, 2014.

[13] H. B. Kekre, "Performance Comparison of Watermarking Using SVD with Orthogonal Transforms and Their Wavelet Transforms," no. March, pp. 1–18, 2015.

[14] G. Gupta, A. M. Joshi, and K. Sharma, "AN EFFICIENT ROBUST IMAGE WATERMARKING BASED ON AC PREDICTION TECHNIQUE USING DCT TECHNIQUE Watermarked image," vol. 9102, no. August, pp. 1055–1059, 2015.

[15] G. V Mane and G. G. Chiddarwar, "Review Paper on Video Watermarking Techniques," vol. 3, no. 4, pp. 1–5, 2013.

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

[17] A. Chitla and C. M. M, "Authenticating Medical Images with Lossless Digital Watermarking," no. April, pp. 291–296, 2014.

[18] S. Dhull, "Digital watermarking," vol. 3, no. 4, pp. 280–283, 2013.

[19] C. Science and M. Studies, "Colored Image Watermarking : A Basis," vol. 7782, pp. 148–152, 2015.

[20] K. Tomar, "International Journal of Advanced Research in Computer Science and Software Engineering A Review Paper of Different Techniques on Digital Image Watermarking Scheme for Robustness," vol. 5, no. 2, pp. 900–904, 2015.

[21] B. Yan, Y. Wang, and L. Song, "Power Spectrum Compliant QIM Watermarking for Autoregressive Host Signals," vol. 6, no. 5, pp. 882–888, 2015.

[22] R. V Mahule, “Analysis of Image Security Techniques using Digital Image Watermarking in Spatial Domain,” no. Nckite, pp. 19–26, 2015.

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

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

[25] K. Ramani, E. V Prasad, and S. Varadarajan, “Protecting Digital Images Using DTCWT-DCT,” pp. 36–44.

[26] R. K. Sheth and V. V. Nath, “Secured digital image watermarking with discrete cosine transform and discrete wavelet transform method,” *2016 Int. Conf. Adv. Comput. Commun. Autom.*, pp. 1–5, 2016.

[27] G. Bhatnagar, Q. M. J. Wu, and B. Raman, “Biometric Template Security based on Watermarking,” *Procedia Comput. Sci.*, vol. 2, pp. 227–235, 2010.

[28] A. U. Islam *et al.*, “An improved image steganography technique based on MSB using bit differencing,” *2016 6th Int. Conf. Innov. Comput. Technol. INTECH 2016*, pp. 265–269, 2017.

[29] R. Gupta and T. P. Singh, “New proposed practice for secure image combing cryptography stegnography and watermarking based on various parameters,” *Proc. 2014 Int. Conf. Contemp. Comput. Informatics, IC3I 2014*, pp. 475–479, 2014.