Watermarking for Images using Alphanumeric Technique

Deepti Varshney, Mamta Bansal, Birendra Kumar Sharma

Abstract: In the current daily routine the sharing of digital content is increasing in large scale through social media. Every individual is sharing his/her activities like photos, message, etc. through social media (i.e. WhatsApp, Facebook, etc.) to other persons without authentication of all these data and through this general activity of people some people are doing fraud to them or misuse of these data or illegally showing to other people without his concern. To ensure the authentication of digital contents this paper proposes methodology to prove the ownership by Digital watermarking and Intellectual Property Right (IPR). This paper explains the concepts of IPR and proposed alphanumeric watermarking technique for authentication of images and its protection from the fraud or misuse. Digital Watermarking has become one of the research areas in many fields from more than decades. This paper gives the methodology of embedding and extraction techniques for images to prove the authentication of images when required its demand. The result of this proposed technique is shown very helpful to society at a globe.

Keywords: Intellectual Property Right(IPR), Copyright, Trademark, Patent, Digital Watermarking, Elliptic Curve Cryptography (ECC)

I. INTRODUCTION

Digital Watermarking and Intellectual Property Right concepts are used to authenticate different multimedia contents to prove the ownership. The word intellect originates from the "intellectus" which means understanding. An intellectual is a person who involves in critical thinking, research and formulating the solution of some social or business-related problems. The intellectual property means the ownership of something intangible with the advent of the knowledge and information technology era like artistic works, symbols, names, images software's used in commerce [9]. Intellectual property rights (IPR) provide an incentive to the creators / researchers to develop his new creation and to share it with other people in the development of the society. The basic aim of the IPRs is to assist in meeting the challenges within the development like reducing poverty, stimulating economic process, improving the health status by providing medicines to the poor, improving access to education and contributing in the sustainable development. Though IPRs provide incentive to the author/creator and lead to a competition in the field of invention but it is also an intellectual protectionism require from theft of these ideas.

   Deepti Varshney* , Department of Computer Science & Engineering, Shobhit University, Meerut, varshney.deepti11@gmail.com
   Dr. Mamta Bansal, Department of Computer Science & Engineering, Shobhit University, Meerut, mamta.bansal@shobhituniversity.ac.in
   Dr. Birendra Kumar Sharma, Department of MCA, AKG Engineering College, Ghaziabad, bksharma888@yahoo.com

The survey released by Business Software Alliance in 2018, it is found that only in IT industries the unlicensed software used by different geographical regions of countries are very high. The unlicensed software used by Central & Eastern Europe and Asia-Pacific is 57 percent, Middle East & Africa is 56 percent, Latin America is 52 percent and North America is 16 percent [10]. The Intellectual property broadly categorized into Industrial property and Copyright.

Industrial property: Industrial property means rights of industrial designs, inventions, trademarks and geographical indications.

Copyright: Copyright means protecting the rights of the creation of human mind in the area of science, art, literature, music, text messages, images, audio-visual etc. and this creative mind peoples called authors, artists, software developers. That is showing the rights or ownership of that individual person who has developed or created new concepts and called intellectual property of that creative mind person. This basic rights of the ownership of intellectual property are known as "intellectual property rights" (IPR). This concept was primarily used in designs, patents, copyrights and trademarks.

This paper presents alphanumeric digital watermarking methodology to protect the authentication of images if multiple person has same copy of images.

II. INTELLECTUAL PROPERTY RIGHTS

According to the World Intellectual Property Organizations, Intellectual Property Rights are categorized into eight categories. The categories are copyright, Patents, Trademark, Integrated Circuits, Breeder's right, Trade secret, Geographical indications and Utility models.

A. Copyright:

The copyright means protecting the rights of creative people like authors, artists etc. for their literary and artistic works. The literary and artistic work may be writing the books, creating the movies & music, making paintings, developing photographs and software. The basic purpose of this is to give the exclusive right to control reproduction or adaptation by others with certain condition. The condition may be permission to use for a certain period of time or charge some amount for sharing knowledge of this technology. The main works covered under copyrights are

➢ Artistic work: It shows the work of a creative painting, drawing, photographs, a sculpture and a work of architecture and any other work of artistic craftsmanship.

- ➢ Literary work: It includes computer programmers, tables and compilations including computer databases.
- ➢ Musical work: Musical work consisting of music and any graphical notation of creative mind people.
- ➢ Dramatic work: It includes any piece of recitation, choreographic work or entertainment in dumb show.
- ➢ Cinematography film: It means any work of visual recording.
- ➢ Sound recording: It means a recording of sound

B. Patent:

Patent is defined as the legal right of an originator to keep out other persons from making or using a discovery. This right is called as 'Intellectual Property Right' and it can be viewed to encouragement of the originator for innovation. In India, the law governing patents is the Patents Act, 1970 ("Patents Act") and continued efforts to comply with its commitment under TRIPS the Patents Act has been amended thrice since 1995, by the Patents (Amendment) Act, 1999 ("First Amendment"), the Patents (Amendment) Act, 2002 ("Second Amendment") and Patents (Amendment) Act, 2005 ("Third Amendment"), Prior to the Third Amendment, the President of India had promulgated Patents (Amendment) Ordinance, 2004 ("Ordinance"), which was later replaced by the Third Amendment. The legislation is supported by the Patents Rule, 2003 ("Rules") [2].

C. Trademark:

A trademark is used to identify and distinguishes the source of the products of one party from those of others, it could be in any form like word, name or symbol. The trademark owner can be an individual, business organization, or any legal entity. For example, trademarks are often displayed on company buildings [15].

D. Integrated circuits:

Integrated circuits is new concepts to give layout to design or topography for integrated circuits in Internet Protocol. It has appeared with many computer technologies. It has implemented through the programming instructions on a computer chip and circuitry printed on semiconductor layers. To implement this concept the design of circuitry on the chip requires great skills, knowledge and money and also needs to be protected as IP [15].

E. Breeder's right:

It is a form of intellectual property rights (IPR) for breeders of new plant varieties. The breeders of new plant varieties are to be protected without their permission against exploitation. As per current breeder's rules a plant breeder's right is granted for 25 years in the case of tree and vines and for all other cases granted only for 20 years.

F. Trade secrets:

A trade secret is used in commercial practice for a non-public and it is part of confidential information. The non-public information is concerning the commercial practices or proprietary knowledge of a business, public disclosure of which may sometimes be illegal. Unlike patents, trade sectors are protected as long as the information is kept secret [15].

G. Geographical indications:

A geographical indication means symbolic sign for a particular region or an items used in specific geographical regions or originated from specific regions or available in only specific reasons. This type of representation generally used with the name of place like brass of Moradabad, Locks of Aligarh, Perfume of Kanauji, Kolhapur chappals of Kolhapur. It is also used for different variety of other products like agricultural. The agricultural products like wheat of MP, Tea of Assam etc.

H. Utility models:

Utility models are related to grant the permission for invention and it was originated from United State of America. An utility model provides exclusive rights to inventor and also allows the inventor to prevent from others to use of commercially without his permission or concern. In India there is no provision of utility models, but patent law exists which does not provide any concepts of utility model like making the rules to make duplicate key machine.

III. DIGITAL WATERMARKING

Digital watermarking introduces the concepts for embedding /extracting the secret information within the content of text documents, images and digital audio and video signals in such a way so that no one can detect it or in other way we can say that it is a process to show an evidence for ownership at the time of demand when any legal issues comes from dispute. This concept is used in various enforcement and protection technique of IPR for text documents, digital images, digital audio, digital video and software's.

The term "digital watermark" was first introduced in 1992 as a "Electronic Water Mark" by Andrew Tirkel and Charles. The term originally used in Japanese as "denshi sukashi" in Japan which was latter pronounced as an "electronic watermark"[13]. Basically, this term was introducing more than 700 years ago as a paper watermarks by different countries to represent brand of papers and the company names where it was produced. After that this invention of paper watermark it was quickly spread over glob to recognize paper and keep its record like date, quality, company name. It also indicates the sizes of original sheets, paper format, quality and strength. This was used as anticounterfeiting measures on money and other documents. They are still widely used as security features in currency today [13].

Digital Watermarking is very helpful to prove ownership/authenticity of text documents, images, copyright notices, verification messages to avoid forgery and security purpose like privacy. In this regard various researchers were proposed different methods. Elliptic Curve Cryptography (ECC) method was used to authenticate the information by generating signature and signed messages [5].

Simple block-based watermarking algorithm in spatial domain was explained [6] and suggested that this technique can be applied in frequency domain to improve the quality. Block based singular value decomposition in spatial & transform domain was proposed for embedding and extraction- reverse of embedding [7]. Techniques for Gray scale conversions were also proposed [8].

IV. THE WORKING PRINCIPLE OF DIGITAL WATERMARKING

A working principal of digital watermarking is a watermark embedding and its recovery system. The system also has a either a public or a secret key to enforce security for prevention of unauthorized parties from manipulating or recovering the watermark. The embedding and recovery processes of watermarking are shown in Fig- 1 and Fig-2.
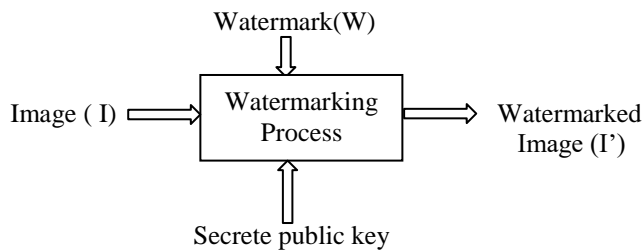
Fig-1: Watermarking embedding process
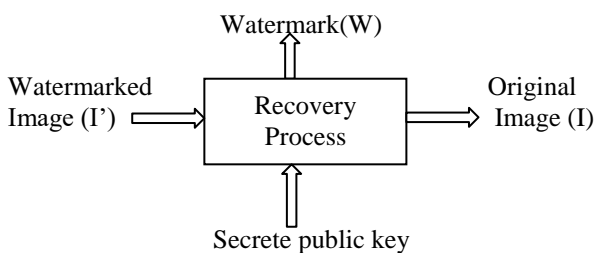
Fig-2: Watermarking Recovery process

V. CLASSIFICATION OF DIGITAL WATERMARKING TECHNIQUES

Digital watermarking techniques can be categorized by the following four criteria [15]

- According to Document
- According to working domain
- According to Human Perception
- According to application

A. According to Document:

The digital watermarking techniques are used according to document in text documents, images, audio and video files are

According to document the digital watermarking in text document are used to prevent the documents like pdf file, doc and other type of text files. In this method the watermarks are inserted in the form of font, shape and the space between characters and line spaces.

According to document the digital watermark in images are used to hide the special information using embedding techniques and it can also be detect or extract by the owners at the time of demand when legal issues required.

According to document the digital watermark in audio files are used in application area of the audio files like MP3, music due to visibility and availability on internet.

According to document the digital watermark in video files are used to control the application by embedding the documents in the form arranging or producing. It is similar and extension of image watermarking. It is used in real time environment for extraction and robustness for compression.

B. According to working domain:

According to working domain the digital watermarking techniques are Least Significant Bit (LSB) and spatial domain [13] for images.

LSB and spatial domain are two different methodology or techniques to embed the watermark in the images and video files. The LSB techniques is the embedding technique which is used to modify the pixel values by changing the LSB position from 0 to 1 and 1 to 0 in defined ways like either in diagonal or in upper triangular position or in lower triangular position or in all pixel. It is also very simple to extract or detect from image when it requires on legal issues. The computation cost of embedding and extraction of this technique is very low, and it is very easy to implement using MATLAB. The spatial domain technique is a patch work technique and based on LSB. In this methodology or technique, the embedding and extraction of the data is similar to LSB but in a patchwork. Its data hiding technique based on either pseudorandom or statistical model. The insertion of a watermark in patch used statistic by a Gaussian distribution.

According to working domain, the other digital watermarking techniques for images and video are Frequency Domain. Frequency Domain (Transform Domain) is a technique in which on certain frequencies some values are altered in the original values. There are three methods to alter the frequencies. The methods are Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Discrete Fourier Transform (DFT) [1][14][16].

The Discrete Cosine Transform is usually used to transforms domains for still digital images. In this method the entire image denotes the coefficients of separate frequencies of cosines and computed by taking 8×8 blocks of the image which are distorted individually in form of two dimension (2D). The resultant of the 2D DCT of an image provides the matrix in which the top left corner denotes lowest frequency coefficient and the bottom right corner denotes the highest frequency coefficient.

Discrete Wavelet Transform is a recent useful technique for digital image processing, digital image compression, watermarking etc. The discrete wavelet transform works according to the time-frequency description for a given signal. Its starts on small waves of frequency called wavelet transform for varying frequency and of limited duration. This wavelet transform again decomposes the image into three spatial orders. The spatial orders are horizontal, vertical and diagonal and it reflects in the anisotropic properties of Human Visual System (HVS). In this system the magnitude of DWT coefficients is larger in the lowest bands (LL) and smallest in the other bands (HH, LH, and HL). In this 2D transform, separate two one-dimensional transforms used in which first is for the image of filtered along the x-dimension using low pass and high pass analysis filters.

Discrete Fourier Transform is a process used to transform continuous event into its frequency components. It is used as the basic of sine and/or cosine multiplied by a evaluating function. It is robust for geometric attacks like scaling, rotation, translation, cropping etc. DFT agrees to processing and analysis of the signal in its frequency domain by analyzing and transforming its coefficients.

C. According to Human Perception:

According to human perception digital watermarking techniques are visible, invisible, dual, robust and fragile watermarking.

Visible watermarking was the simplest and most fundamental way of watermarking. In this technique embedded watermarks are visual when the contents are viewed.

Invisible watermarking is used to embed secret data as digital data in images, audio or video but it is not possible to identified easily. The invisible watermark is a concealed image which cannot be seen by human eyes, but it can be detected by using detection algorithm. This watermark is used to proof the ownership at time of demand as legal issues. It can be used as a backup of visible watermark.

Dual watermarking technique is a method of combining both visible and invisible watermark in the inside of the conceal.

Robust watermarking is a method of embedding technique which does not affect the modification of the watermarked content. It means that describes only those watermarks which cannot be detected within an object. It is not always possible but can give just the probability of availability of watermark. It is possible when if the tampering level is too high and automatically modified from the original. In this situation the quality will degraded. To maintain the quality, we can define some limits of the embedded watermark for the maximum required robustness. In this watermark technique the extraction algorithm should produce accurate watermark, even after the strong modifications.

Fragile watermarking technique is a technique in which watermark gets damaged if watermarked content is modified or manipulated. It has potentially to displays selective robustness which generally called fragile watermark. It is useful for tamper-proofing.

D. According to application:

According to application digital watermarking techniques are source based and destination-based watermarking.

Source based watermarking technique is useful when the owner of a document wants to distribute to multiple destinations with the same secrete key or authentication information. This technique is used for authentication purpose only to identify whether the received document is tempered or not.

Destination Based Watermarking technique is useful when the owner of a document wants to distribute to multiple destinations with the different secrete key or authentication information which is embedded behind the document. In this technique only legal receiver can open the document and it is very useful to prevent illegal reselling of the document.

VI. IPR AND DIGITAL RIGHTS

IPR and digital rights are two different important aspects while sharing the data in the globe. We want to share the data with our own rights without any modification, but some people are doing forgery and modifying or changing the data regularly without concern to owner of the data in today digital age. The IPR and digital rights play important roles when legal issues come for where the unauthorized data shared, how the data has modified, what data has shared and modified, when data has shared and modified. The major issues are

➢ Similar or identical data production by others without permission or concerned
➢ Data production in another different form
➢ Denying accepting copied data
➢ Refused to accept from where data has originated
➢ Digital Data distributed in different countries through world wide web
➢ Easy to reprint and distributing a copyrighted data or book
➢ IP law is constantly changing or updating as per upcoming new technologies.

VII. WAYS FOR PROTECTION OF DIGITAL / INTELLECTUAL PROPERTY

In current digital age multiple ways has defined to protect our digital or intellectual property. The most common method are Digital Rights Management (DRM) and Technical Protection Measures (TPM).

The DRM technologies is also called Electronic Rights Management Systems. It is used to ensure the copyrights via protecting and identifying the content. It is also used for ensuring access for permissible work and controlling its payment. It is very useful to prevent from illegal users to access the content and this can be done with some protection technologies like user ID & password and term & condition of license agreements.

The other technology used for protection of digital content is Technical Protection Measures (TPM). It is useful for companies who are working to produce text, music and video. This technology is used for securing and protecting content of text, music and video from unauthorized use. The DRM and TRM technologies sometimes used together like If an author wants to charge fee for his or her published work in legal way then DRM technology required to get fee. These technologies are increasingly employed to distribute and sell content over the Internet. The other useful technologies are

A. Cryptography:

It is the oldest technology to ensure privacy and security of digital information over Internet. This is an encryption technology for the digital information and the encrypted information is unable to understand due to conversion of information from one form to another form. It requires decryption technologies for decrypt the data to get in actual form. It means this technology is useful only at the time of transmission or distribution.

B. Digital Signature Technology:

In this technology the identity of the sender and / or receiver can includes like sending date & time, receiving date & time or any unique code etc. and added with digital information. This additional information with original information indicates the delivery of information on write time and also authenticate to write person. It is also useful for to prevent illegal copying.

C. Electronic Marking:

Electronic marking technique is system generated unique mark that is associated with each of the document copies.

It is also used to protect copyrights. It is mainly used at the time of publishing electronic documents like printing faxed data etc.

D. Security Features of Operating System:

The security and integrity features of each OS is unique. The few features of windows 10 are Cortana on Desktop, Xbox App, Improved Multitasking, Universal Apps, Continuum. Similar MS-SQL Server has some unique feature like it handle any amount of data and high performance.

VIII. APPLICATIONS OF DIGITAL WATERMARKING

The major applications of the digital watermarking and its purpose are shown in below table

Application	Purpose of Watermarking
Owner Identification	Prevent unauthorized copying
Proof of ownership	Identification of authorized user
Copy and Playback Control	Protection from duplication
Medical applications	To verify the reports like X-ray and MRI reports
DVD protection and access control	Prevent unauthorized copying
Fingerprinting	Track back a malicious user
Copy protection	Prove ownership
Copyright protection	Prevent access to unauthorized users
Video Authentication	Ensure that the original content has not been altered
Broadcast monitoring	Identify the video being broadcast and check usage

IX. PROPOSED ALPHANUMERIC METHODOLOGY

An alphanumeric methodology used to embed the watermark in images by using either only numeric values or alphabets. This concept is known to only a person who is embedding the watermark in images. It is very useful for all type of images which are shared by persons and on demand that person can show his authentication through extraction of watermark from images. The graphical representation of embedding and extraction is shown in fig-3 and fig-4:
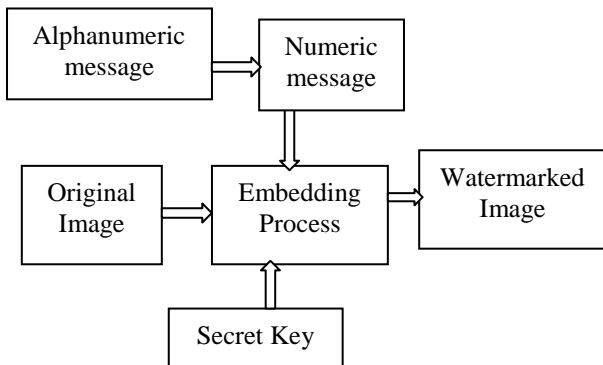
Fig.-3 : Block diagram of an Embedding process
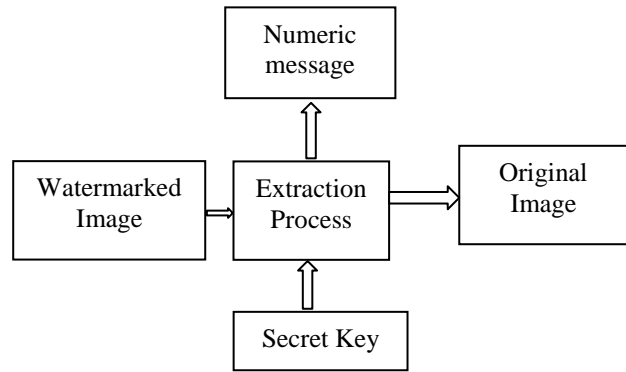
Fig-4: Block diagram of an Extraction process

The algorithm for proposed embedding processes are

- ▢ Read the Input/original image
- ▢ Read the alphanumeric message and secret key
- ▢ Extract numeric digit from alphanumeric message
- ▢ Embed the Input image and numeric message
- ▢ The resultant image is watermarked image

The algorithm for proposed extracting processes are

- ▢ Read the watermarked image and secret key
- ▢ Use extraction procedure
- ▢ The resultant is watermark (i.e. Numeric message) and original image
- ▢ Show the alphanumeric message if required

X. EXPERIMENTAL RESULTS

The experimental results of proposed algorithm are shown below:
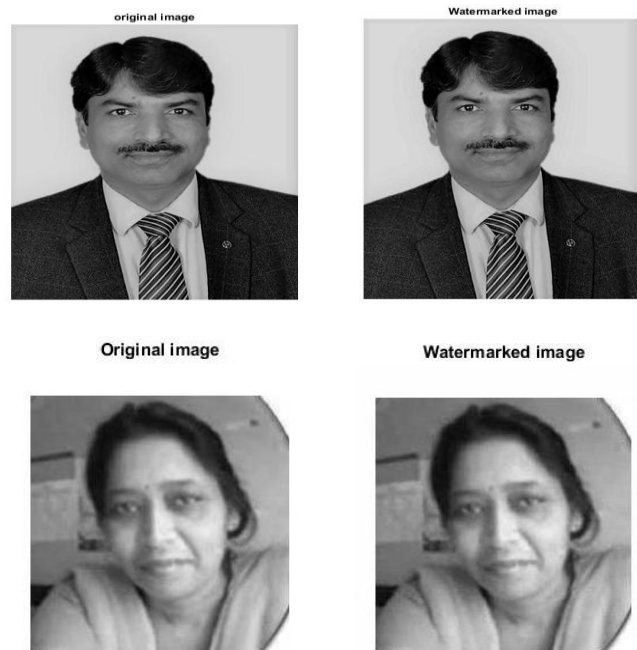
Original image

Watermarked image

XI. ANALYSIS OF PROSED METHODOLGY

The proposed algorithm is more secure than previous algorithm because it uses multi-level approach to embed the algorithm using LSB technique. In this approach in first level only numeric value is extracted from text messages containing numeric and alphabet characters that is numeric and text part are separated to each other's. The separated numeric part will start from 0 to 9 numeric value and will contains some length. The extracted numeric part is different for different users. The extracted numeric part has embedded in original images using LSB techniques starting from first numeric value of extracted numeric part in either continuation or alternate in either rows, columns or diagonals. This information knows only creator and attacker will not able to identify embedding techniques or information embedded in the original images. In the next level LSB technique is used because it is invisible and less time require to change the least significant bits and not possible to identify by human beings. This proposed methodology is more robust and very effective to share images with watermark in globe and easily proven by originator of originality of images when required its demands.

The possible attacks on embedded images are subtractive distortion and additive attacks.

Subtractive Attacks: It is used when the attacker will remove watermark from the image. In the proposed methods watermarks are embedded in such a manner so that if an attacker remove the watermark then the some portion of an image will reflect different from original which identified easily in changes of an image, which will prove by creator the original image has been changed by attacker and the originality will shows by extraction algorithm.

Distortion Attacks: It is used when the attacker damages the watermark in such a way so that creator or owner cannot be prove its originality. In the proposed method multilevel embedding technique has been proposed so it is not possible for attacker to damage the watermarks.

Additive Attacks: It is used when the attacker insert its own new watermarks instead of damage or changing the watermarks. It can be either replace the original watermark or get inserted in addition to the original watermark. Therefore, it is difficult to prove which watermark was inserted first. In the proposed method if attacker insert some new watermark or replace with the new watermark the orininal image will change and on demand it will be proven for originality with proposed methodology.

XII. CONCLUSIONS

In this paper we have represented the Intellectual Property Right and Digital Rights of digital information with its related issues and techniques. The issues are associated with the usage of digital information like article, e-journals papers, incompatible hardware and software, graphics, scholarly recognition and obsolescence. In digital environment it is difficult to define a boundary between what is permissible to up to which extent and what is infringement. Today in the age of digital information very difficult to judge for fair use, fair access and fair control the infringement of copyright law. It is almost impossible for a copyright owner to know which person used his/her work. The copyright protection should be encouraging the creativity and not for creating hurdles in the use of information. Therefore, there is need of more research for the free flow of information between the owners of copyright and the users of the information. All these are possible with the help of methods defined by Intellectual Property Right and Digital Watermarking. This paper proposed the methodology used for Intellectual Property Right with alphanumeric Digital Watermarking which are very helpful for persons who are sharing images on social media and want to always in the form of it originality.

REFERENCES

1. Himanshu Rastogi and B. K. Sharma, "A Study on Intellectual Property Right and Digital Watermarking", International Journal of Advanced Research in Computer Science, Volume 8, No. 7, July – August 2017, ISSN No. 0976-5697

2. Nishith Desai Associates, Intellectual Property Law in India, July (2015)

3. http://eprints.uthm.edu.my/6936/1/MOHAMED_ABDISALAN_SAID.pdf

4. http://eprints.rclis.org/28939/1/Intellectual%20Property%20Rights%20in%20Digital%20Environment_ISI.pdf

5. Arathi Chitla, M. Chandra Mohan, "Authentication of Images through Lossless Watermarking (LWM) Technique with the aid of Elliptic Curve Cryptography", International Journal of Computer Applications (0975 – 8887) Volume 57– No.6, November 2012

6. Peyman Rahmati, and Andy Adler, and Thomas Tran. "Watermarking in E-commerce", International Journal of Advanced Computer Science and Applications,Vol. 4, No. 6, 2013

7. Rania A. Ghazy, Alaa M. Abbas "Block-based SVD image watermarking in spatial and transform domains" , International Journal of Electronics, 2015 Vol. 102, No. 7, 1091–1113

8. Malli B, Lagishetty Mounica, Nandhitha.N.M ,Balamurugan.V, "Development of efficient Quality Preserving Invisible Watermarking Technique to embed both Images and Data in an Image" IEEE Online International Conference on Green Engineering and Technologies (IC-GET), 2016,

9. https://www.wipo.int/edocs/pubdocs/en/intproperty/450/wipo_pub_450.pdf

10. https://gss.bsa.org/wp-

content/uploads/2018/05/2018_BSA_GSS_Report_en.pdf

11. Lalit Kumar Saini & Vishal Shrivastava, "A Survey of Digital Watermarking Techniques and its Applications", International Journal of Computer Science Trends and Technology (IJCST), Volume 2 Issue 3, PP- 70-73, May-Jun 2014.

12. Prabhishek Singh, R S Chadha ,"A Survey of Digital Watermarking Techniques, Applications and Attacks",International Journal of Engineering and Innovative Technology (IJEIT), Volume 2, Issue 9, March 2013

13. Monika Patel,Priti Srinivas Sajja and Ravi K. Sheth, "Analysis and Survey of Digital Watermarking Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 10, PP 203-210, October 2013

14. M.Hariharalakshmi, Dr. M.Sivajothi, Dr.M.Mohamed SathikInternational "Survey of Digital Watermarking techniques for Data security" Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, Issue 3, March 2017

15. B.K.Sharma "Watermarking for copyright protection of software codes" A Ph.D. Thesis, 2012

16. Sunil Kumar Vishwakarma, B. K. Sharma, Syed Qamar Abbas, "Digital Watermarking for Image uthentication using Spatial-Scale Domain based Techniques" IJRTE, ISSN: 2277-3878, Volume-8 Issue-4, November 2019

AUTHORS PROFILE

Dr. Birendra Kumar Sharma, is a HoD (MCA) of Ajay Kumar Garg Engineering College, Ghaziabad. He has obtained his MCA degree from JNU, New Delhi, M.Tech. from Guru Gobind Singh Indraprastha University, Delhi and Ph.D. from Shobhit University, Meerut. His areas of specializations are Digital Watermarking, Steganography & IPR. During his career of 20+ years of experience in the academic he has published 10 books for UG & PG students of engineering like Discrete Mathematics, Theory of Computation, Computer concepts and programming in C etc. and more than 24 research papers in International/National Journals/Conferences.

Dr. Mamta Bansal, has been in the field of Technical Education for the last 30 years. Mamta Bansal received her Ph.D. (Computer Engineering & Information Technology) in 2013 from Shobhit University, Meerut. Currently she is working as an Professor in Shobhit University, Meerut. Her research interest includes Data Mining, Web Mining, Crawler, Cloud Computing and Programming Languages. She has about 40 papers on her credit, which have been published in International, National Journals of repute and presented in various Conferences. She has guided many B.Tech., M.Tech., MCA, M.Phil. and Ph.D. students for their dissertation, project report works.

Ms. Deepti Varshney, is HoD (Computer Science) at SRCOE, Pune. She has completed her M. Tech. from UPTU, Lucknow. She is pursuing Ph. D. from Shobhit University, Meerut. Her research area is Digital Watermarking.