A Fundamental Study of Digital Image Watermarking

Shubham Godhar[1], Vyom Kulshreshtha[2]

[1]M Tech Scholar, Department of Computer Science, Dr. APJ Abdul Kalam Technical University, Lucknow, Uttar Pradesh, India
[2] Assistant Professor, Department of Computer Science, Sachdeva Institute of Technology, Mathura, Uttar Pradesh, India

Publication Info

Article history:
Received : 14 February 2020
Accepted : 23 May 2020

Keywords:
Cryptography, Digital watermarking, Discrete cosine transform (DCT), Embedding, Hidden, Images.

Corresponding author:
Vyom Kulshreshtha
e-mail: *vyom19@gmail.com*

Abstract

As the use of the internet is at peak nowadays, with which people do communicate and interact with the things easily. Such a kind of use of the internet creates a huge demand for the safety and protection of data. For such safety and security purpose, techniques like water making, cryptography, etc. introduced. With the help of these techniques, we can protect digital data. This survey will represent various aspects of digital watermarking like characteristics of watermarking, types of watermarking technique, merits and demerits, applications, kinds, embedded, and extraction process. Different algorithms will be considered while performing digital watermarking like discrete wavelet transform (DWT), singular value decomposition (SVD), etc. For securing e-governance applications, this survey will be useful for further researches and studies in implementing watermarking techniques.

1. INTRODUCTION

As you are seeing, a large amount of data is transmitted every day in the form of audio, video, or any digital form through the internet. This transmission of data takes place with the help of information and communication technology it is very easy for attackers or users to copy, store, delete, or to modify the data. Such properties of data allow the attackers to use the data or media illegally. So, one of securing data is digital watermarking from such unauthorized use of data. We can use this technique for all digital media like documents, images, audio, videos, etc.

In this method, the creator's identification mark (watermark) is merged with the digital media at the sender as well as the receiver's end too.

While comparing digital watermarking with traditional watermarking, in digital watermarking, the signals can be audio, video, 3D models, pictures, or text, while in traditional water, marking the media is like video or images. With the rapid and speedy hands-on with technology accessing speed of data overuse of internet-breaking the bars. While noticing this, requirement of protecting the copyright is at demand like anything, which is done by using the digital watermarking technique. There are two interests of these techniques:

- Documents digitations
- Untroubled traffic

2. STAGES OF DIGITAL WATERMARKING

The digital watermarking technique is the way of embedding the given water to make information into conservative information, and while choosing the conservative information from the watermarked information human cognitive system cannot receive it.

For example, the possessory name, symbol, or signature will conserve in the video, audio, images, etc.

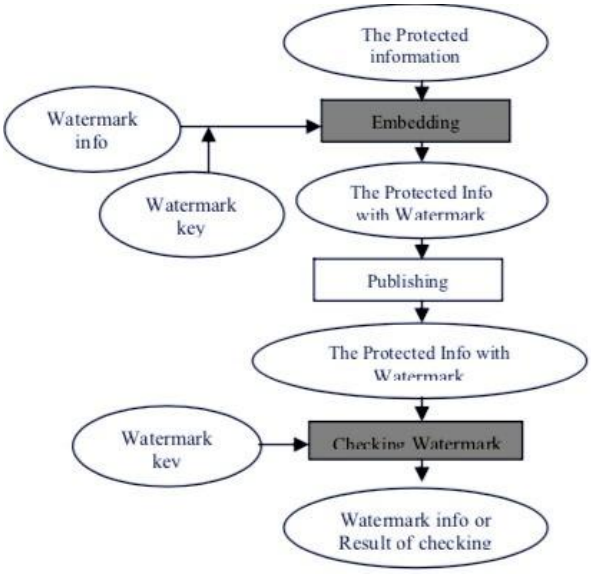

Fig. 1: Fundamental process of digital watermarking[1]

2010-2019 S-JPSET : Vol. 12, Issue Supplementary-1, ISSN : 2229-7111 (Print) and ISSN : 2454-5767 (Online)

3. FUNDAMENTAL PROCESS AND STEPS IN WATERMARKING

The complete watermarking process is considered in three different stages as:

3.1. Generation and Embedding

There are some sequences that are used in the digital watermarking technique is like the pseudo-random number, m-sequence, and chaotic sequence. [5] To understand the inserting process, do understand the combination of the watermark signal and the original picture.

3.2. Distribution and Possible Attacks

With the help of the transmission of signals through the watermark channel, we can see the distribution process. The attacks on the broadcast channel can be intentional or accidental.

3.3. Detection

With the help of the detection process, the creator can easily identify and provides the required details and data to the expected receiver. These are of two kinds: [5]

- Informed detection
- Blind detection

4. FEATURES OF DIGITAL WATERMARKING

This division depicts the characteristics of advanced watermarking estimation:

- *Imperceptibility*: Crucial requirement of advanced watermarking is to have the watermarked picture should simulate the other alike as the original picture. This insists that there is not much distortion on the original picture. The installed watermark sought not to be common to the human eye. To calculate the nuance, by and enormous peak signal to noise ratio (PSNR) is used.
- *Security*: The watermarking framework sought to be checked. For example, the programmer sought not to be in a condition to eliminate the watermark without having the learning of embedding estimation. The watermarking framework must be fit for the same against all Incursions. Incursion attempt to withdraw, change, or used into the watermark. Incursions are fundamentally ordered in two different types, for example, latent incursion and dynamic incursion. Uninvolved incursion just recognizes the watermark data, while dynamic incursion attempts to change the watermark data.
- *Robustness*: The capability of the strength of watermark nearby to both authentic and unauthentic incursion is baffle as strength. Robustness depends upon watermarks data limit, deceivability, and quality. For the most part, an ethical watermarking estimation sought to be detailed against channel preparation, noise enlargement, geometrical changes, for example, revolution, scaling, interpretation, and loss pressure, for example, JPEG pressure.
- *Scope*: Scope of the watermarking framework depicts embedding extreme measures of watermark data in single information. The extreme limit of embedding data in information can be determined by bargaining either intangibility or power of estimation.
- *Multiplicity*: The time and exertion expected to enter and recovered the watermark data are called as multifaceted nature of the watermarking framework. The mind-boggling estimation in the watermarking framework required more programming and equipment affirms to execute it that brings about evaluating the estimation cost. To lower the computational expense of the watermarking framework, it should be minimum puzzling. Information less puzzling watermarking estimations is executed.
- *Invariability*: This feature of an improved watermarking framework depicts the similarity of creating rare information during the eradication technique for watermarking.[5]

5. ATTACKS IN DIGITAL WATERMARKING

A loss in the signal can also be caused by the transmission media, which is implied by a damaged content. These attacks may be intentional or accidental.[6]

- *Removal and Interference Attacks*: From the watermarked object, the watermarked data is segmented. Such attacks abuse the fact that the watermark is usually an additive noise present in the host signal.
- *Geometric Attacks*: This attack is basically used to manipulate the watermarked object. The operation is done in such a way that a detector can't find the watermarked data, but the demerit is that it is bounded with images or videos.
- *Cryptographic Attacks*: If we compare the above two attacks, i.e., Geometric and removal with the cryptographic attack, the third attack works with the breaking of security of data, while the above two attacks do not breach the security.
- *Protocol Attacks*: These attacks abuse the gaps in the watermarking concept. One example of such an attack is the IBM attack. [8] The IBM attack is also known as the deadlock attack, inversion attack, or fake-original attack. [10]

6. IMAGE WATERMARKING

Image watermarking is defined as it is the method where the creator's copyright identification is embedded with the host image. It is quite interesting to know when and how

 2010-2019 S-JPSET : Vol. 12, Issue Supplementary-1, ISSN : 2229-7111 (Print) and ISSN : 2454-5767 (Online)

the very first watermarking technique is used. At Bologna, Italy, in 1282, this method was used very firstly.

Then the uses and implementation of techniques kept on raising in paper mills as a trademark of the company. Then this technique use was common in practice up to half of the 20th century. Various other fields where it was used were—

- Postage stamps
- Currency notes

Steganography is the way of hiding of digital data with other content so that secure transmission of digital data takes place. Digital watermarking is derived from the same word. Still, some difference is between both the terms.

6.1. Process of Watermarking an Image

Two kinds of watermarking techniques are listed below:

- In the host image, the embedding of the watermark.
- From the given image, extraction of the watermark.

In this process, the watermark is embedded in a host image at the source, i.e., at the time of creating an image. This process is shown in Fig.3.

By using the same embedding algorithm as in the above process, a watermark can also be extracted from an image—this process is shown in the following figure.

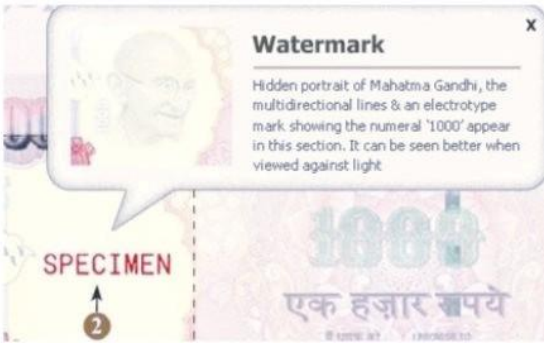

Fig. 2: Watermark on Indian currency [3]

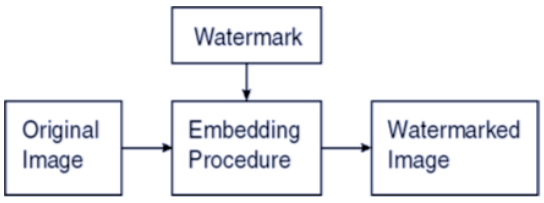

Fig.3: Embedding process of image watermarking [3]

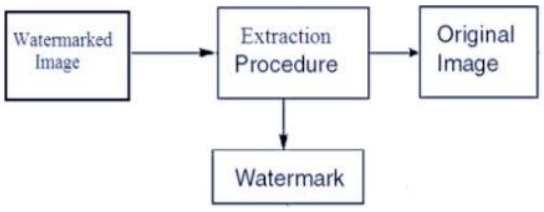

Fig.4: Extraction process of watermark [3]

7. WATERMARKING TECHNIQUES

In a rapidly growing digital era, watermarking has caught the eye of so many stakeholders and researchers for various reasons. It carries enough superfluous information that could be used to embed watermarks.[2] For protecting the data, watermarking contains different techniques and methods.

There are two domains in which watermarking techniques work. These two domains are dimensional and transform.[8] In comparison to transform watermarking, dimensional watermarking is much easier and is less resource consuming. Thus its computing speed is higher than transform, but it is less susceptible to frequent attacks. The dimensional techniques can be easily applied to any image.

The most important method is the lower significant bit (LSB).

7.1. Lower Significant Bit (LSB)

The LSB is the easiest dimensional watermarking technique to insert a watermark in the minimum controlling bits in selected pixels of the cover image.

Various steps should be followed in inserting a watermark in the host picture by using LSB: [4]

- Firstly, the RGB image will be converted into a greyscale image
- Two-time accuracy of the image should be prepared
- Shuffling of the impactful bit at low impact place
- Make the least noteworthy bits of original picture null.
- Add edited version (step 3) of a watermarked image to a modified (step 4) host image.

The main advantage of this method is that it can be comfortably performed on images, and it provides high perceptual clarity.

7.2. Additive Watermarking

A bogus random noise pattern can be inserted in the pixels of the picture. These noise pattern can be in integers or in floating form. For assuring watermark detection, the noise is created by a key, such that the correlation between the numbers of different keys will be very low. [5]

7.3. Spread Sprectrum Modulation Based Technique (SSM)

In this technique, the generated energy at one or various frequencies knowingly spread in time. This technique embeds information by linearly merging the original image with small spurious signals. This is regulated by an embedded watermark.

7.4. Mapping Texture Way

Images which has texture part, this technique will work only with such kind of images, and the watermark is hidden in the texture part of the image with a large number of

2010-2019 S-JPSET : Vol. 12, Issue Supplementary-1, ISSN : 2229-7111 (Print) and ISSN : 2454-5767 (Online)

the arbitrary texture image, this algorithm. Will work and disadvantage is that this method cannot work automatically. With a continuous pattern of the image, data is hidden.

7.5. Patchwork Algorithm

This method is based on an analytical model in which data is hiding way developed by Bender et al. In this, we insert with particular probability using Gaussian distribution. In this spurious two patches should be selected and named them F and B E. Image of F patch data are brightened, and the image of patch E data-id darkened.

7.6. Correlation-Based Technique

In this technique, a pseudo-random noise (PN) pattern says W (x, y) is added to cover image I (x, y). Iw (x, y) = I (x, y) + k × W (x, y). Where K represents the gain factor, Iw represents a watermarked image at position x, y, and I represent the cover image. By increasing the gain factor, the robustness of watermark can also be increased, but the quality of the watermarked image will decrease.

The watermark is inserted in the spectral coefficients of the image, and thus frequency domain techniques are widely applied in comparison to dimensional domain technique. The most implemented transforms are discrete cosine transform (DCT), discrete Fourier transform (DFT), and DWT. Characteristics of the human visual system are better captured by the spectral coefficient, and thus this is also the reason for which frequency-domain method is more applicable than dimensional domain method. Some of the main algorithms of frequency-domain methods are discussed below

- *Discrete Wavelet Transform (DWT):* Discrete wavelet transform algorithm; the picture is divided into four parts:
  - Horizontal part
  - Corner to corner part
  - Vertical part
  - Estimation part
- The isolation is done for changing into a lower resolution goals pictures. The method is repeated to figure out number scale wavelets declining. This strategy of watermark performs all calculations in all respects.
- *Discrete Cosine Transform (DCT):* In discrete cosine transform, we install the watermark on the picture with the help of utilizing numerous calculations as this algorithm is very quick as the contrast with different strategy while applying DCT, the watermark is implanted on the inside recurrence group on account of the deterioration of picture.
- *Discrete Fourier Transform (DFT):* In discrete Fourier transform algorithm, the edge which is watermarked is gotten, and, in the process, the co-productive magnitude is engaged while performing backward additionally connected. Merits of this algorithm are it is more powerful and improvise.

8. VARIOUS WORKS DONE IN THE FIELD

During this research by Monika Patel et al., [6] focus was on the portrayal that the advanced information is anything but difficult to alter and modify. While measuring this issue, the concept of watermarking is evaluated. In this, the data analyzed along with copyrights or validations are implanted on very first information that keeps the information from unapproved get to. Various algorithmic estimations can be utilized for installing the watermark on the information. The choice of estimation relies on the idea of the information.

During this author, Bhattacharjee T et al. [7] characterizes a technique implemented for information stowing away and sharing mutually. In this, above all else, the picture is partitioned into little offers, and afterward, these offers are implanted into the spread picture to conceal the information. Inserting of that information is done in the DCT region that utilizes M-cluster distributed range balance. This is a practically equivalent to strategy as (k, n) plot covertly sharing.

As mentioned in this paper by Vinita Gupta et al., [8] it is featured that it is a way to obscure the details and data over any picture, sound, video, and so forth; it is like cryptography. Watermarking is clarified in this paper's image.

During the present scenario, Preeti Parashar et al., [9] put forward that generally, information disseminates over the internet with the definition of getting connected or in terms of communication. The fundamental concern will be the security of computerized information. In this, the advanced watermarking is working to check the undisclosed knowledge. It keeps the information from replication by obscuring the intricate text in the data and details. The areas arranged the strategy of picture watermarking as dimensional space; change space and so forth dimensional area is a system that chips away at the premise of pixels. Also, space, recurrence area deals with the changing area of the picture. During the paper author mainly mentioned the dimensional and change area alongside their points of presentation and difficulties.

The creation of a technique by Miroslav Dobsicek, [10] which has the object is encoded with one key and cannot be scrambled along with few various keys, the connected entropy among scramble and one explicit decode key.

Built-up of online verification framework by Yusuk Lim, Changsheng Xu, and David Dagan Feng, 2001. [11] If there should arise an occurrence of a watermark inserting

 2010-2019 S-JPSET : Vol. 12, Issue Supplementary-1, ISSN : 2229-7111 (Print) and ISSN : 2454-5767 (Online)

framework that is introduced in the server as an application programming that any approved client, who approaches the server, can create a watermarked picture. The conveyance can utilize any sort of system transmissions, for example, FTP, email, and so forth when the picture is conveyed to remotely, customers can access to validation site page to obtain a check of the picture.

Another strategy which controls "flappable" pixels to implement explicit square-based relationship to insert a lot of information without causing observable ancient rarities by Min Wu and Bede Liu, June 2003, proposed. [12] The shrouded information would then be able to be extricated without utilizing the first picture and can likewise be precisely separated after great printing and filtering with the assistance of a couple of enrolment marks.

During the year 2007, there was a proposal for information security by Nameer N. EL-Emam that utilize the LPB inclusion steganographic technique. During the implementation of this technique, layers with good securities have been designed through three layers to make it hard to get through the encryption of the information and befuddle steganography too. [13]

A clarification is provided by Rehab H. Alwan, Fadhil J. Kadhim, and Ahmad T. Al-Taani, 2005, that strategy with three fundamental advances. In the first place, the picture's edge is identified utilizing Sobel veil channels. Second, the minimum huge piece LPB, of every pixel is utilized. At last, a dim level network is connected utilizing a fluffy technique, and the American Standard Code for Information Interchange (ASCII) code is utilized for data covering up. The earlier piece of the LPB speaks to the edged picture after dim level network, and the staying six bits speak to the first picture with almost no distinction conversely. The given technique implants three pictures in a single picture and incorporates, as an exceptional instance of information installing, data stowing away, recognizing, and validating content inserted inside the computerized pictures. [14]

In the year 2008, Prof S. K. Bandyopadhyay, Debashis Ganguly, Swarnendu Mukherjee, Debnath Bhattacharyya, and Poulami Das has proposed a heuristic way to deal with conceal tremendous measure of information utilizing LPB steganography technique. The final stego-picture was contortion less. Additionally, they have given much accentuation on space multifaceted nature of the information concealing technique. [15]

During the year 2008, a strategy chips away at more than one picture utilizing the idea of document hybridization presented by G Sahoo and R K Tiwari. This strategy executes cryptographic techniques to implant two various data records utilizing steganography, and because of this reason, they have utilized a stego key for the installing procedure. [16] The embedding of high-entropy information (regularly because of encryption) changes the histogram of shading frequencies in an anticipated manner. Along these lines, to get greater security in our recommended technique, we have inserted a whole picture over another picture of double the size of the target picture for the surprising change in the previous picture.

During the information implementation of this paper, the strategy is proposed to assure computerized personality reports against a print scan incursion for the verified Identification (ID) card confirmation framework by Peyman Rahmati, Thomas Tran, and Andy Adler—watermarking in e-business. [17] The current Print-Scan (PS) task forces a few bends, for example, geometric revolution and histogram mutilation on the watermark area, which may cause the loss of data.

During this paper, another technique for sorting watermark procedure through picture displaying is examined by Neil F. Johnson, Sushil Jajodia, and Zoran Duric. [18] The picture displaying called alpha channel syntheses utilizes a steady veil. Two pictures with level cover and slow veil are utilized to make a watermark, which changes dim estimations of that exact pixel in the image. The technique for watermark recuperation by applying the converse change to contorted pictures appears. The image is watermarked utilizing the variant of Digimarc's Image Mark watermarking channel that is accessible with Adobe Photoshop, and the image is contorted by using the Starmark instrument of relative change.

During this paper, estimation for installing watermarking is displayed by utilizing DWT and encoded with QR codes by Vinita Gupta and Atul Barve. [19] At this point spread image is chosen, and DWT is attached to it. A key X is selected to produce the QR code as a mystery key. Quick Response (QR) code and watermark pictures are scrambled with the help of the XOR task. At that moment, the scrambled watermark is inserted into the spread image, and backward DWT is attached to the implanted watermark image. In support of extraction, essentially use the DWT on the spread image. This estimation is very basic in view of the utilization of straightforward X-OR task for encoding. This estimation is appropriate on various sorts of incursion on watermarked images like JPEG compression, Performance Network Analyzer (PNA), salt, Poisson Noise (PN), and Gaussian Noise (GN).

9. CONCLUSION

Numerous papers are investigated with respect to the watermarking and its strategies. Every procedure that is considered some of them is a progression in customary systems, and some are bases for new proposed strategies. Every technique is effective and has numerous favorable

2010-2019 S-JPSET : Vol. 12, Issue Supplementary-1, ISSN : 2229-7111 (Print) and ISSN : 2454-5767 (Online)

circumstances; however, on the contrary, there are a few hindrances too. There are numerous sorts of watermarking accessible. Digital watermarking is plainly unmistakable to the end client, while undetectable digital watermarking is not noticeable to the end clients. Undetectable watermarking must be uncovered by utilizing a few estimations or systems. The works considered in the overview have taken any a couple of considered powerful prerequisites of the watermarking past, which the instruments are to be chosen like they can convey every single real necessity of the computerized watermarking. For more thought, the things can be considered for the satisfaction of the real necessities of the computerized watermarking like invisibility, security, efficiency, and robustness.

10. REFERENCES

[1] L. K. Saini, V. Shrivastava, "A Survey of Digital Watermarking Techniques and its Applications", IJCST, Vol. 2, pp. 70-73, 2014.

[2] S. Singla, R. Bansal, "Watermarking Techniques for User Selection System as Noticeable and Unnoticeable Using DWT", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Vol. 3, Issue 5, pp. 1743-1746, May 2014.

[3] M. Patel, P. S. Sajja," Analysis and Survey of Digital Watermarking Techniques," ijarcsse, Vol 3, pp 203-210, 2013.

[4] V. Gupta, "A Review on Image Watermarking and Its Techniques," IJMEIT, Vol. 2, Issue 1, January 2014.

[5] Dobsicek, M., "Extended steganographic system," 8th Intl. Student Conf. on Electrical Engineering, FEE CTU 2004, Poster 04.

[6] S. Dhiman, O. Singh, "Analysis of Noticeable and Unnoticeable Image Watermarking – A Review", International Journal of Computer Applications, Vol. 147, No.3, pp. 36-38, August 2016.

[7] T. Bhattacharjee, S. P. Maity, H. K. Maity, "Progressive quality access through secret sharing and data hiding scheme", International Image Processing, Applications and Systems Conference, pp 5- 7, 2014

[8] P. Parashar, R. K. Singh, "A Survey: Digital Watermarking Techniques," International Journal of Signal Processing, Image Processing and Pattern Recognition, vol 7, no. 6, pp. 111-124, 2014.

[9] Nalluri, S. K., & Parasaram, V. K. B. (2016). Early Approaches to Robotic Process Automation in Enterprise Systems. International Journal of Humanities and Information Technology, 1(01), 12-28. https://doi.org/10.21590/ijhit.01.01.06

[10] Parasaram, V. K. B., & Nalluri, S. K. (2016). A Comparative Analysis of Risk Management Frameworks in Enterprise IT Projects. SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology, 8(02), 147-155. https://doi.org/10.18090/samriddhi.v8i2.7149

[11] Y. Lim, C. Xu, and D. D. Feng, "Web-based Image Authentication Using Innoticeable Fragile Watermark," Pan- Sydney Area Workshop on Visual Information Techniqueing (VIP2001),Sydney, Australia, pp. 31 -34, 2001.

[12] M. Wu and B Liu, "Data Hiding in Binary Image for Authentication and Annotation", IEEE Trans. Image Techniqueing, vol. 6, Issue 4, pp. 528-538, Aug. 2004.

[13] Nameer N. EL-Emam "Hiding a enormous amount of data with high security using steganography algorithm," Journal of Computer Science, pp. 223–232, April 2007.

[14] Rehab H. Alwan, Fadhil J. Kadhim, and Ahmad T. Al-Taani, "Data Embedding Based on Better Use of Bits in Image Pixels," International Journal of Signal Techniqueing, Vol 2, No. 2, pp. 104-107, 2005.

[15] S. K. Bandyopadhyay, D. Bhattacharyya, S. Mukherjee,D. G., Poulumi Das, "A Secure Scheme for ImageTransformation," IEEE SNPD, pp. 490–493, August 2008.

[16] G. Sahoo, R. K. Tiwari, "Designing an Embedded Algorithmfor Data Hiding using Steganographic." International Journal of Computer Science and Network Security, Vol.8 No.1, pp. 228-233, January 2008

[17] P. Rahmati, A. Adler, and T. Tran, "Watermarking in E-commerce," (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 4, No. 6, 2013.

[18] Neil F. Johnson, Zoran Duric, and Sushil Jajodia. "A Role for Digital Watermarking in Electronic Commerce," ACM Computer Survey, 1999

[19] V. Gupta, A.Barve, "Robust and Secured Image Watermarking using DWT and Encryption with QR Codes," International Journal of Computer Applications (0975 – 8887), Vol. 100, No.14, August 2014.

AUTHORS

Shubham Godhar, have done my schooling from RamanlalShorawala Public School, Mathura. Thereafter, I went to GLNA, Mathura (Affiliated to UPTU, Lucknow)for doing my B.Tech in Computer Science and completed it in 2014. In 2015 I enrolled in M.tech from SIT, Agra (Affiliated to UPTU, Lucknow), and left the course in middle because of some personal issues. Now, I am committed to complete my M.tech.

Vyom Kulshreshtha, Have Twelve years of experience in Industry and academics. Presentlyworkingas Assistant Professor in Department of Computer Science at Sachdeva Institute ofTechnology, Mathura, Uttar Pradesh. Have published 10 research papers in InternationalJournals, and 5 research papers

in National conferences. Key research field are DigitalImage Processing, Distributed Systems, Soft computing Techniques and ArtificialIntelligence.

2010-2019 S-JPSET : Vol. 12, Issue Supplementary-1, ISSN : 2229-7111 (Print) and ISSN : 2454-5767 (Online)