International Journal of Modern Communication Technologies & Research (IJMCTR)
ISSN: 2321-0850, Volume-1, Issue-6, August 2013

A Survey of Digital Watermarking Techniques

Neha Singh, Mamta Jain, Sunil Sharma

Abstract—**The enormous popularity of the World Wide Web in the early 1990's demonstrated the commercial potential of offering multimedia resources through the digital networks. Since commercial interests seek to use the digital networks to offer digital media for profit, they have a strong interest in protecting their ownership rights. Since the threat of using multimedia information, digital forgeries, and unauthorized sharing (piracy) of digital content have increased among content creators, distributors and users. Today multimedia information piracy alone has subjected all the industries to multi-billion revenue losses. Traditional digital content protection techniques, such as encryption and scrambling, alone cannot provide adequate protection of copyrighted contents, because these technologies are unable to protect digital content once they are decrypted. One way to discourage illegal duplication is to insert information known as watermark, into potentially vulnerable data in such a way that it is impossible to separate the watermark from the data. Digital watermarking is the process of inserting a digital signal or pattern inside a digital image, which provides evidence of authenticity. This paper presents a survey on various information hiding techniques and describes classification of digital Watermarking techniques.**

Index Terms— Copyright Protection, Embedding, Information Hiding, Watermarking.

I. INTRODUCTION

Editing, distribution and reproduction of the private digital multimedia are becoming extremely easier and faster with the existence of the internet and the availability of pervasive and powerful multimedia tools. The problems of illegal duplication, fake currency, business security, protecting intellectual property etc. are becoming more and more important. Digital watermarking has emerged as a possible method to tackle these issues. Digital images are the most popular carrier file format among various available formats like audio files, video files, and text files because of their frequency on the Internet. Until now, intellectual property and value has always been bound to some physical container that could not be easily duplicated, thereby guaranteeing that the creator benefits from his work. Therefore information hiding techniques plays a vital role for providing copyright authentication.

II. HISTORY OF INFORMATION HIDING

In ancient times, the messages were sent on foots. There are only two options to hide a message: hide it on the messenger, or have the messenger memorize it.

Manuscript received 20 August, 2013.

Neha Singh, Department of Electronics & Communication Engineering, Institute of Engineering & Technology, Alwar, India.

Mamta Jain, Department of Electronics & Communication Engineering, Institute of Engineering & Technology, Alwar, India.

Sunil Sharma, Asst. Professor, Department of Electronics & Communication Engineering, Pacific Institute of Technology, Udaipur.

The practice and idea of information hiding has a long history. According to Greek historian Herodotus around 440 B.C., the famous Greek tyrant Histiaeus [1]-[3], while in prison, used to send message to his son-in-law by shaving the head of his trusted slave to tattoo a message on his scalp. He dispatched the slave with the hidden message when the hair grew back.

The second story also came from Herodotus, which says that a soldier named Demeratus [1] used wax-covered tablet to send a message to Sparta that Xerxes intended to invade Greece. He removed the wax from the tablet and wrote the secret message on the underlying wood and then recovered the tablet with wax to make it appear as a blank tablet and finally sent the document without being detected.

Hiding messages using invisible ink was also very popular. Ancient Romans used to write their secret messages between the blank lines by invisible ink that is generally prepared by fruit juices, milk, and urine etc. When heated, the invisible ink would darken and becomes visible. Ovid in his "Art of Love" suggests using milk to write invisibly. During World War II, it was also reported that the Nazis [3] invented several information hiding methods such as Microdots, and have reused invisible ink and null ciphers. As an example a message was sent by a Nazi spy that read:

''Apparently neutral's protest is thoroughly discounted and ignored. Isman Hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils.'' By collecting the 2nd letter from each word the secret message reveals:

''Pershing sails from NY June 1''

The monk Johannes Trithemius, founders of modern cryptography, described an extensive system for concealing secret messages within innocuous texts in his three volume work Steganographia, written around 1500. Later in 1665 Gaspari Schott wrote a four hundrerd pages book Steganographica from the idea of Trithemius. Further in 1883, Auguste Kerchoffs' published Cryptographie militaire which is mostly about cryptography. But during twentieth century the information hiding techniques actually came into existence.

III. DISCIPLINES OF INFORMATION HIDING

A wide range of problems beyond the embedding messages in content have been encircled by the general term Information *hiding* (or *data hiding*). The term *hiding* can refer to either for information secrecy (Steganography) or information imperceptibility (Watermarking). Two important sub disciplines of information hiding are Watermarking and Steganography [4] that are closely related to each other but with different underlying properties, requirements and designs, thus result in different

technical solutions. The general disciplines of information hiding [1], [3]-[9] are given in figure 1.

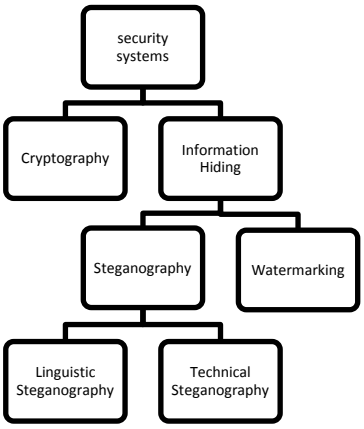

Fig. 1. Different Disciplines of Information Hiding

A. Cryptography

The term cryptography stands for "secret writing". It is the study of methods of transmitting messages in different form so that only the intended recipients can remove the disguise and read the message. The message that we want to convey is known as "plain text" and the disguised message is termed as "cipher text". Enciphering or encryption is the process of converting plain text to cipher text and deciphering or decryption is the reverse process of encryption that converts the cipher text to plain text. The block diagram of cryptography [1] is given in figure 2.

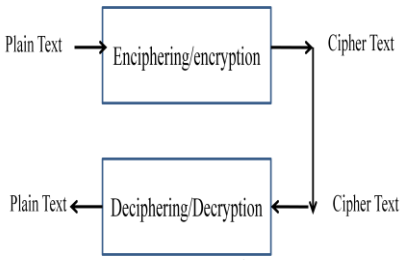

Fig. 2. Block Diagram of Cryptography

There are many methods have been developed to encrypt and decrypt the messages in order to keep them secret. Cryptography [1], [2], [7] keeps the content of message secret but it is unable to keep the existence of message secret. It also requires secret transmission. Encryption procedure mainly aims at protecting the image (or other kind of data) [10] during its transmission. Once decrypted, the image is not protected any more. Once the presence of hidden information is revealed or even suspected, the purpose of Steganography is partly defeated. The strength of Steganography can thus be amplified by combining it with cryptography.

B. Steganography

The word Steganography [1], [2], [4], [7], [8], [11-15] is derived from the Greek words "*stegos*" meaning "cover" and "*grafia*" meaning "writing" defining it as "covered writing". The information is hidden exclusively in images in Image Steganography. Steganography is the art of science of invisible communication. It hides the secret information in other information in such a manner such that hidden information appears nothing to human eye. Figure 3 shows the generic model of Steganography.

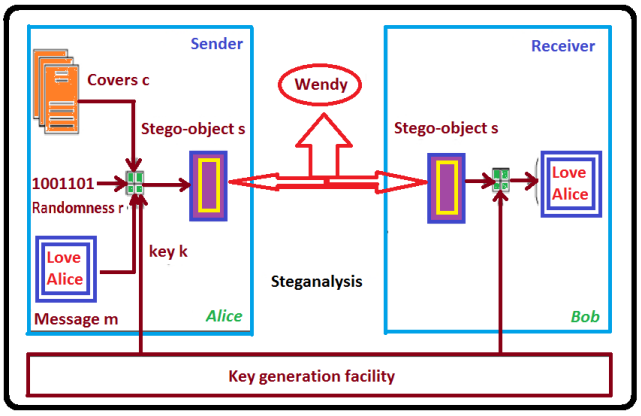

Fig. 3. The Generic Model of Steganography

The Steganography techniques are classified as Technical and Linguistic Steganography. The former, such as invisible ink tries to hide data physically while the later one uses linguistic or language forms of hidden writing. Linguistic Steganography, also called acrostic was one of the popular ancient Steganography techniques. The secret messages were encoded as initial letters of sentences or successive tersest in a poem. These are the semagrams and the open code. A semagram is a secret message that is not in a written form.

C. Watermarking

Digital watermarking [4] can be defined as the process of embedding a certain amount of information (technically known as watermark) into multimedia content including text documents, images, audio or video streams, such that the watermark can be detected or extracted later to make an assertion about the data. It allows a person to provide hidden copyright notices or other verification licenses.

IV. Comparisons of Steganography, Watermarking and Cryptography

Steganography is usually applied to a one-to-one relationship and it is a two-way communication. Information is hidden by one individual for another individual to decode. Watermarking is usually applied to a one-to-many relationship and the communication is one-way. Since Steganography, watermarking and Cryptography are the three interlinked techniques but different [13] in several aspects which are given below:

i) Watermarking mainly prevents illegal copy or claims the ownership of digital media but it is not geared for communication

ii) Cryptography scrambles the data to be communicated so that unintended receivers cannot perceive the information. However, the fact that the communication has been carried out is known to everyone.

iii) Steganography transmits data by actually hiding the existence of the message so that a viewer cannot

detect the transmission of message and hence cannot try to decrypt it.

The comparison [3] between these three techniques is summarized in table 1.

Criterion/method	Steganography	Watermarking	Cryptography
Carrier	Any digital media	Mostly image & audio files	Usually text based, with some extension to image files
Secret Data	Payload	Watermark	Plain Text
Key	Optional	Optional	Necessary
Detection	Blind	Usually informative (i.e. original cover or watermark is needed for recovery)	Blind
Result	Original with imperceptible changes	Original with imperceptible changes	Cipher text
Objective	Secret Communication	Copyright preserving	Data protection
Concern	Capacity	Robustness	Robustness
Type of Attacks	Steganalysis	Image Processing	Cryptanalysis
Visibility	Never	Sometimes	Always
Fails when	It is detected	Removed/Replaced	De-ciphered
Flexibility	Free to choose any suitable cover	Cover choice is restricted	N/A
History	Very ancient except its digital version	Modern era	Modern era

TABLE 1 COMPARISON OF STEGANOGRAPHY, WATERMARKING AND CRYPTOGRAPHY

V. A DETAILED LOOK AT WATERMARKING

Digital Watermarking is the process of embedding information into digital multimedia content (audio, video, or still images) such that the information can later be extracted or detected for a variety of purposes including copy prevention and control. This technique provides a solution to the longstanding problems faced with copy-righting digital data. A general definition [16] can be given to watermarking is:

!"Hiding of a secret message or information with an ordinary message and the extraction of it at its destination!"

Unlike cryptography, after any decryption process, watermarking allows the protection of the data. It embeds secret information in such a way that appears negligible to Human eye (i.e. without affecting the visual content of image). This process avoids degrading original digital product and utilizes the limitation of Human Visual System (HVS) to make the watermark invisible.

The basic watermarking algorithm [17] is divided in two steps: first one is watermark embedding and other one is watermark detection/extraction. If I is the original image (cover image) and W is the watermark and F( ) denotes the embedding function then the watermark image I' can be written as:

$$I' = F(I, W) \qquad 1.1$$

Basic approach is that from original image I a property sequence is extracted i.e. V = v1, v2,…,vN, corresponding to watermark sequence W = w1, w2,….,wN. W is embedded into V according to certain model to obtain the adjusted sequence V' = V + W = v'1, v'2,….,v'N. Replace V by V' to get the watermarked image I'.

If X( ) denotes the extraction function then recovered watermark can be expressed as:

For blind detection

$$W' = X(I') \qquad 1.2$$

For non-blind detection

$$W' = X(I', I) \qquad 1.3$$

If the correlation function C (W, W') > = T (Where T is threshold value)

Then the recovered watermark is correct otherwise it is destroyed by transmission/transformation.

The Basic Watermarking system is usually consists of three different stages, embedding attack and detection which is shown in Figure 4. In embedding stage the watermark is embedded into host object to produce a watermarked signal. Then transmitted during which it may get a modification called an attack. In detection the watermark is extracted from the attacked signal. The embedding is done by manipulating the content of host image in spatial domain or transform domain. Sometimes a key is added in watermarking process to authenticate the legal copy right holder.

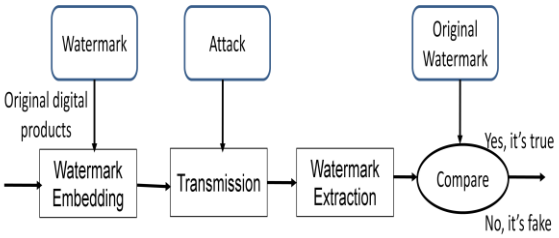

Fig. 4. General Model of Watermarking

VI. Classification of Digital Watermarking

Digital watermarking is possible just because of that Human vision system (HVS) is not perfect. Digital watermark uses the limitation of HVS to make it invisible, thus do not degrade original digital products, as well being hard to get identified or destroyed. This technique provides a solution to the longstanding problems faced with illegal replications of digital data. Currently digital watermarking technique can be broadly classified in five categories on the basis of various aspects [3]-[5] as shown in figure 5 which are discussed further.

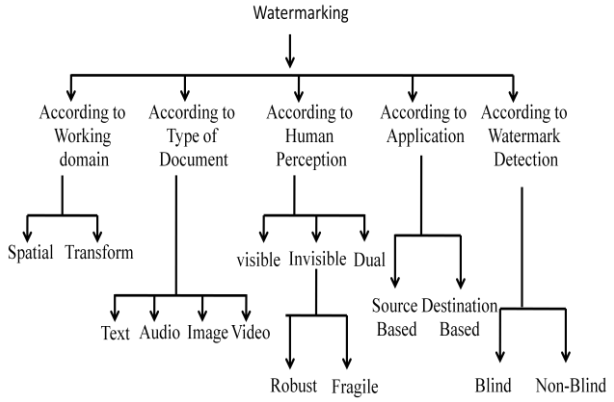

Fig. 5. Classification of Digital Watermarking

According to type of document

On the basis of digital file format used for watermarking, it can be classified in four categories:

1) Text watermarking
2) Image watermarking
3) Audio watermarking
4) Video watermarking

The formats which provide a high degree of redundancy are more suitable for embedding. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display. Redundant bits [2] are those bit that can easily be modified without affecting the object. Generally image and audio file is used which comply with this requirement while researchers have also uncovered other two file format used for information hiding. Images are quite popular cover or carrier objects used for watermarking. Many different image file format exist in digital domain, most of them for specific application.

According to Working Domain

Another way to classify watermarking is by how the watermark is embedded in the cover image [18]-[23], it can be embedded either in Spatial domain or in transform domain. The first watermarking scheme was introduced in spatial domain. Perceptual information about the image can easily be got by some image analysis operation (e.g. edge detection) which is then used to insert a watermark, directly in the intensity values of predetermined regions of images. It is the simplest method of inserting a watermark but don't show robustness to common image alterations.

Another way is transform domain in which firstly original image is transformed into frequency domain by the use of any method like Discrete Fourier Transform, Discrete Cosine Transform, Discrete Wavelet Transform, or Hybrid Transform. Then watermark is added to the transform coefficient of original image. Finally the inverse of corresponding transformation is done to get watermarked image.

The compatibility of Human Visual System (HVS) is an additional advantage in transform domain technique. Table 2 shows a small comparison between spatial domain and transform domain watermarking.

Parameter	**Spatial domain**	**Transform domain**
Computational Cost	Low	High
Robustness	Fragile	More Robust
Perceptual Quality	High control	Low Control
Capacity	High (depend on the size of the image)	Low
Example of Applications	Mainly Authentication	Copy Rights

TABLE 2 COMPARISONS BETWEEN SPATIAL AND TRANSFORM DOMAIN TECHNIQUES

The comparison shows that the main advantage of embedding the watermark in transform domain is that the transform domain based technique will be more robust compared to spatial domain which is the basic requirement of watermarking.

According to Human Perception

Based on Human perception, watermarking techniques [2], [5], [8], [18] can be divided into four categories:

1) Visible Watermarking
2) Invisible Robust Watermarking
3) Invisible Fragile Watermarking
4) Dual Watermarking

In Visible watermarking the secondary translucent overlaid into the primary content and appears visible on a careful inspection. Visible watermark are intentionally perceptible to human observer. Visible watermarking is used to prevent unauthorized access to an image and also act as an advertisement. An example of such watermarking is shown in figure 6 which shows a visible watermark in a French 15th century Genesis excerpt, created by IBM Vatican Library project.

Fig. 6. An Example of Visible Watermarking

In invisible watermarking, the watermark is embedded into the image in such a way that it cannot be perceived by human eye. It is used to protect the image authentication and prevent it from being copied. The embedded watermark can be extracted or detected later to identify the owner or the origin of the host image, yielding relevant information as well. The presence of invisible watermark should not interfere with the work being protected. Invisible watermarking is further categorized as robust or fragile [4], [5], [8].

In fragile watermarking if the file is modified, then the watermark is easily destroyed. It can be really useful in judiciary process for example where it is imperative to be certain that what is used is genuine. In contrast robust watermark are unaffected despite of various attack, it can resist attack. It means the mark should be embedded in the most perceptually significant components of the object [5].

In Dual watermarking two watermarks are embedded instead of one for increased protection and security one is visible and other one is invisible. An invisible watermark is used as a backup for the visible watermark as an example: sign can be embedded in invisibly manner while logo can be embedded in visible manner. The concept of Dual watermarking is shown in figure 7 which shows that first visible watermark is added to the original image and then in visible watermarked image the invisible watermark is embedded.

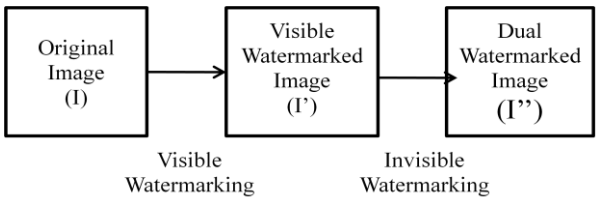

Fig. 7. Concept of Dual Watermarking

According to Application

From application point of view the watermark can be source based or destination based. Source-based watermark are desirable for ownership identification or authentication where a unique watermark identifying the owner is introduced to all the copies of a particular image being distributed. A source-based watermark could be used for authentication and to determine whether a received image or other electronic data has been tampered with. The watermark could also be destination based where each distributed copy gets a unique watermark identifying the particular buyer. The destination -based watermark could be used to trace the buyer in the case of illegal reselling.

According to Watermark Detection/Extraction

Depending on the combination of inputs and outputs [17], [18] watermarking is classified as blind or non-blind techniques. Non-blind watermarking technique requires original image for the detection of watermark while blind technique do not use original image for extracting the watermark. The advantages of non-blind technique are lower error probability, higher capacity and tracking transaction but it may lead to multiple claims of ownership.

VII. Conclusion

One can see that there exists a large selection of approaches to hide information in images. All the major file formats have different methods of hiding messages, with different strong and weak points respectively. Watermarking is the process of hiding some data or information in an appropriate multimedia file as for example image, audio and video files. It comes under the evidence that if the feature is visible, the chances of attack is evident, thus the goal of invisible watermarking is always to conceal the very existence of the embedded data. It has been propelled to the forefront of current security techniques by the remarkable growth in available digital media via World Wide Web. Watermarking technology plays an important role in securing business as it allows placing an imperceptible mark in the multimedia data to identify the legitimate owner.

References

[1] Sabu M Thampi, "Information Hiding Techniques: A Tutorial Review", *ISTE-STTP on Network Security & Cryptography, LBSCE*, 2004.
[2] Kanzariya Nitin K., Nimavat Ashish V., "Comparison of Various Images Steganography Techniques", *International Journal of Computer Science and Management Research,* Vol. 2, Issue 1, ISSN 2278-733X, pp 1213-1217, January 2013.
[3] Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt, "Digital Image Steganography: Survey and Analysis of Current Methods", *Proceeding of Signal Processing 90*, pp 727–752, 2010.
[4] Yusnita Yusof, Othman O. Khalifa, "Digital Watermarking For Digital Images Using Wavelet Transform", *Proceedings of the IEEE International Conference on Telecommunications and Malaysia International Conference on Communications*", 1-4244-1094-0, pp 665-669, May 2007.
[5] Fabien A. P. Petitcolas, Ross J. Anderson, Markus G. Kuhn, "Information Hiding – A Survey", *Proceeding of IEEE, Special Issue on Protection of Multimedia Content, 87(7),* ISSN 1062-1078, pp 1062-1078, July 1999.
[6] Niels Provos, Peter Honeyman, "Hide and Seek: An Introduction to Steganography", *Published by the IEEE Computer Society*, ISSN 1540-7993, pp 32-44, May-June 2003.
[7] Deepa S, Umarani R, "A Study on Digital Image Steganography", *International Journal of Advanced Research in Computer Science and Software Engineering"*, Volume 3, Issue 1, ISSN: 2277 128X, pp 54-57, January 2013.
[8] R.Poornima, R.J.Iswarya, "An Overview of Digital Image Steganography", International Journal of Computer Science & Engineering Survey (IJCSES), Vol.4, No.1, pp 23-31, February 2013.
[9] Sushil Kumar, S.K.Muttoo, "A Comparative Study of Image Steganography in Wavelet Domain", *International Journal of Computer Science and Mobile Computing, IJCSMC*, Vol. 2, Issue 2, ISSN 2320–088X, pp 91 – 101, February 2013.
[10] Vallabha VH, "Multiresolution Watermark Based on Wavelet Transform for Digital Images", *Multiresolution watermarking of Digital Images,* Cranes Software International Limited.
[11] A.Nag, S. Biswas, D. Sarkar, P.P. Sarkar, "Novel Technique for Image Steganography Based on Block-DCT and Huffman Encoding", International Journal of Computer Science and Information Technology, Volume 2, Number 3, June 2010.
[12] K.B.Raja, C.R.Chowdary, Venugopal K R, L.M.Patnaik, "A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images", *IEEE Proceeding of Image and Signal Processing session 5B*, 7803-9588, pp 171-176, 2005.
[13] Blossom Kaur, Amandeep Kaur, Jasdeep Singh, "Steganographic Approach for Hiding Image in Dct Domain", *International Journal of Advances in Engineering & Technology, IJAET*, Vol. 1,Issue 3, ISSN 2231-1963, pp 72-78, July 2011.

[14] Souvik Bhattacharyya, Gautam Sanyal, "A Robust Image Steganography using DWT Difference Modulation (DWTDM)", *International Journal Computer Network and Information Security*, pp 27-40, July 2012.
[15] H S Manjunatha Reddy, K B Raja, "High Capacity and Security Steganography using Discrete Wavelet Transform", *International Journal of Computer Science and Security (IJCSS)*, Volume 3, Issue 6, pp 462-472.
[16] Feng Liu, Yangguang Liu, "A Watermarking Algorithm for Digital Image Based on DCT and SVD", *IEEE Congress on Image and Signal Processing*, 978-0-7695-3119-9, pp 380-383, 2008.
[17] Liu Lin, "A Survey of Digital Watermarking Technologies", Unknown.
[18] Suhad Hajjara, Moussa Abdallah, Amjad Hudaib, "Digital Image Watermarking Using Localized Biorthogonal Wavelets", *European Journal of Scientific Research*, Vol.26, No.4, ISSN 1450-216X, pp 594-608, 2009.
[19] Jih Pin Yeh, Che-Wei Lu, Hwei-Jen Lin, and Hung-Hsuan Wu, "Watermarking Technique Based on DWT Associated with Embedding Rule", *International Journal of Circuits, Systems and Signal Processing*, Issue 2, Volume 4, 2010.
[20] Santhi K, Anil Kumar M N, "Biometrics based Steganography using Circular Folding in DWT Domain", *International Journal of Computer Applications*, Volume 61, No.10, ISSN 0975 – 8887, pp 47-51, January 2013.
[21] Yedla dinesh, Addanki purna ramesh, "Efficient Capacity Image Steganography by Using Wavelets", *International Journal of Engineering Research and Applications (IJERA)*, Vol. 2, Issue 1, ISSN 2248-9622, pp 251-259, Jan-Feb 2012.
[22] Mei Jiansheng, Li Sukang, Tan Xiaomei, "A Digital Watermarking Algorithm Based on DCT and DWT", *Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09) Nanchang, P. R. China*, ISBN 978-952-5726-00-8, pp 104-107, May 22-24, 2009.
[23] A. M. Kothari, A. C. Suthar, R. S. Gajre, "Performance Analysis of Digital Image Watermarking Technique-Combined DWT-DCT over individual DWT", *International Journal of Advanced Engineering & Applications*, pp 177-181, Jan 2010.

Neha singh is presently working as an Assistant Professor in Institute of Engineering & Technology, Alwar. She has completed her Degree of B.E. from Rajasthan University in the year 2004 and M.Tech. from MNIT, Jaipur in the year 2009. She has an experience of more than 9 years in the field of teaching & Research. She has published 19 papers in International/National Conferences/Journals. She has guided PG students in the area of Steganography, Image Mosaics and Gesture recognition. She is lifetime member of International Association of Computer Science & Information Technology. Presently she is also working on World Bank Project under MHRD.

Mamta Jain received her B.E. in Electronics & Communication Engineering from Rajasthan University in 2008. She is a M.Tech. student at Institute of Engineering & Technology, Alwar. Her area of interest is Digital Image Watermarking.