# Review of Digital Watermarking System: A Robust Method for Protection

[1]Sangeeta Madhesiya., [2]Shakil Ahmed
[1]*Associate Professor, Department of Mathematics*
*Doon Institute of Engineering & Technology, Shyampur, Rishikesh, Uttarakhand, India*

[2]*Research Scholar*
*Faculty of Science and Technology, CMJ University Megalaya , India*

***Abstract*— In the present scenario of global network of Internet, we want to save our digital data i.e. audios, videos, pictures, texts and so on. For this reason we need a security system. In the field of security system for securing the data on Internet there are many systems. But in the present paper we discussed about the security or protection of these data (audio, video, pictures, texts or 3D models) by using digital watermarking and we try to define different applications, techniques, characteristics, uses, growth and challenges of digital watermarking. Digital watermarking is a promising technology to embed information as unperceivable signals in digital contents. Various watermarking techniques have been proposed to protect copyrights of multimedia digital contents over Internet trading so that ownership of the contents can be determined in subsequent copyrights disputes. We propose a singular value decomposition method, SVD method can transform matrix A into product $USV^T$, which allows us to refactoring a digital image in three matrices. The using of singular values of such refactoring allows us to represent the image with a smaller set of values, which can preserve useful features of the original image, but use less storage space in the memory, and achieve the image compression process. It makes use of intelligence user certificates to embed the identity of the users into the intelligence documents to whom are distributed. In particular, keeping the identity secrecy between document providers and users (but yet traceable upon disputes) is a key contribution of this protocol in order to support for intelligence applications.**

## I. INTRODUCTION

A **digital watermark** is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of computer-aided information hiding in a carrier signal; the hidden information should, but does not need to contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently used for tracing copyright infringements and for banknote authentication. Like traditional watermarks, digital watermarks are only perceptible under certain conditions, i.e. after using some algorithm, and imperceptible anytime else. If a digital watermark distorts the carrier signal in a way that it becomes perceivable, it is of no use. Traditional Watermarks may be applied to visible media (like images or video), whereas in digital watermarking, the signal may be audio, pictures, video, texts or 3D models. A signal may carry several different watermarks at the same time. Unlike metadata that is added to the carrier signal, a digital watermark does not change the size of the carrier signal.

The needed properties of a digital watermark depend on the use case in which it is applied. For marking media files with copyright information, a digital watermark has to be rather robust against modifications that can be applied to the carrier signal. Instead, if integrity has to be ensured, a fragile watermark would be applied.

Watermarking can be considered as a special technique of stegnography where one message is embedded in another and the two messages are related to each other in some way. The most common examples of watermarking are the presence of specific patterns in currency notes which are visible only when the note is held to light and logos in the background of printed text documents. The watermarking techniques prevent forgery and unauthorized replication of physical objects. Digital watermarking is similar to watermarking physical objects except that the watermarking technique is used for digital content instead of physical objects. In digital watermarking a low-energy signal is imperceptibly embedded in another signal. The low-energy signal is called watermark and it depicts some metadata, like security or rights information about the main signal. The main signal in which the watermark is embedded is referred to as cover signal since it covers the watermark. The cover signal is generally a still image, audio clip, video sequence or a text documents in digital format.

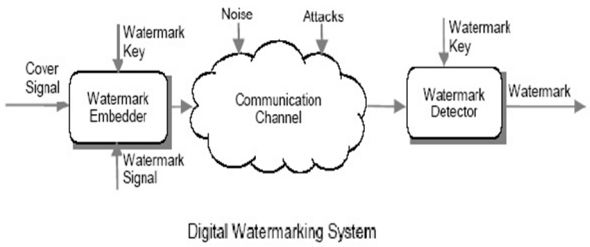


Fig. 1 Digital Watermarking System

The digital watermarking system essentially consists of a watermark embedder and a watermark detector. The watermark embedder inserts a watermark onto the cover

signal and the watermark detector detects the presence of watermark signal. Note that an entity called watermark key is used during the process of embedding and detecting watermarks. The watermark key has a one-to-one correspondence with watermark signal (i.e., a unique watermark key exists for every watermark signal).The watermark key is private and known to only authorized parties and it ensures that only authorized parties can detect the watermark. Further, note that the communication channel can be noisy and hostile (i.e., prone to security attacks) and hence the digital watermarking techniques should be resilient to both noise and security attacks.

Digital watermarking is a technique for embedding a watermark into a digital image to protect the owner‘s copyright of the image. The embedded watermark in the resulting stego-image must be robust because the stego-image may be rotated or scaled by illicit users. It is desirable that after such rotation or scaling attacks, the watermark is not fully destroyed and can still be extracted to verify the copyright of the image. Many watermarking techniques for copyright protection have been proposed in recent years.

Digital watermarking technology makes use of the fact that the human eye has only a limited ability to observe differences. Minor modifications in the color values of an image are subconsciously corrected by the eye, so that the observer does not notice any difference.

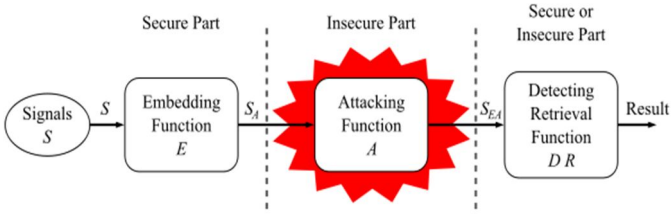


Fig. 2 Digital watermarking life-cycle phases

General digital watermark life-cycle phases with embedding-, attacking-, and detection and retrieval functions.

The information to be embedded in a signal is called a digital watermark, although in some contexts the phrase digital watermark means the difference between the watermarked signal and the cover signal. The signal where the watermark is to be embedded is called the host signal. A watermarking system is usually divided into three distinct steps, embedding, attack, and detection. In embedding, an algorithm accepts the host and the data to be embedded, and produces a watermarked signal.

Then the watermarked digital signal is transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. While the modification may not be malicious, the term attack arises from copyright protection application, where third parties may attempt to remove the digital watermark through modification. There are many possible modifications, for example, lossy compression of the data (in which resolution is diminished), cropping an image or video or intentionally adding noise.

Detection (often called extraction) is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, then the watermark still is present and it may be extracted. In *robust* digital watermarking applications, the extraction algorithm should be able to produce the watermark correctly, even if the modifications were strong. In *fragile* digital watermarking, the extraction algorithm should fail if any change is made to the signal.

## II. HISTORICAL DEVELOPMENT OF DIGITAL WATERMARKING

The term “watermark” was probably originated from the German term “wassermarke”. Since watermark is of no importance in the creation of the mark, the name is probably given because the marks resemble the effects of water on paper.

Watermarks are identification marks produced during the paper making process. The first watermarks appeared in Italy during the 13th century, but their use rapidly spread across Europe. They were used as a means to identify the papermaker or the trade guild that manufactured the paper. The marks shown here were created by a wire sewn onto the paper mold. Watermarks continue to be used today as manufacturer's marks and to prevent forgery.

The term "digital watermark" was first coined in 1992 by Andrew Tirkel and Charles Osborne.

We undertook to implement this system as a software application rather than as hardware for a good reason. Once something is implemented in hardware, it becomes very difficult to change or modify the algorithm. However, digital watermarking technology is still very much in a process of development, so we felt it would be better to give customers watermarking capability while preserving as much flexibility as possible. It was also important to give customers the ability to use this capability on an ordinary computer that can be acquired anywhere. We also sought to develop an application that can apply digital watermarking to any and all kinds of digital content, because the day is fast approaching when marking digital materials with a watermark will be regarded as entirely natural and commonplace.

Using digital watermarks for copyright protection is only one application example. For example, digital watermarking has excellent market potential for implementing content management systems, and many other potential applications. Or if video clips and photographs were marked with watermarks and one had the ability to search for content based on watermark, extremely interesting databases could be created. Usual index is outside of the content, but watermarking technology offers the possibility of such index incorporated right in the content itself. This suggests that there are other novel ideas and applications for digital watermarking that have yet to be discovered.

Recently we have seen the emergence of an application where people take pictures with their cell phone cameras and go to a special website, but this too might be considered a type digital watermarking application. We have not quite reached the stage where digital watermarking has penetrated into our

everyday lives to provide enormous utility and convenience. But there is little doubt that eventually digital watermarking will emerge as a core technology in society, and this is certainly one thing that drives and inspires us to further efforts in developing and refining this technology. There is much to look forward to!

The rapid growth of the Internet increased the access to multimedia data tremendously. The development of digital multimedia is demanding as an urgent need for protect multimedia data in internet. Digital watermarking technique provides copyright protection for digital data. The digital watermarking technique is proposed as a method to embed perceptible or imperceptible signal into multimedia data for claiming the ownership. A digital watermark is a piece of information which is embedded in the digital media and hidden in the digital content in such a way that it is inseparable from its data.

## IV. TYPES OF WATERMARKING

There are two famous approaches to watermarking that are mostly used.

***Spatial Domain Watermarking:*** Spatial domain watermarking is easy to implement and requires no original image for watermark detection. However, it often fails under signal processing attacks such as filtering and compression [10]. Besides, the fidelity of the original image data can be severely degraded since the watermark is directly applied on the pixel values.

***Transform Domain Watermarking:*** Watermark embedded in the transform domain e.g., DCT, DFT, wavelet by modifying the coefficients of global or block transform. Frequency domain watermarking generally provides more protection under most of the signal processing attacks. But the existing frequency-domain watermark algorithms require the original image for comparison in the watermark retrieval process, which is not practical for a huge image database. Furthermore, the necessity of progressive transmission is one of the requirements for Internet distribution. The lack of progressive transmission property in existing spatial- and frequency-domain watermarking algorithms limits their Internet applications. There are a number of transforming techniques like DCT (Discrete Cosine Transform), DFT (Discrete Fourier Transform) FFT (Fast Fourier Transform). We have used the DWT (Discrete Wavelet Transform).

## III. APPLICATIONS OF DIGITAL WATERMARKING

***Owner Identification:*** Digital watermarking can also be used for owner identification to identify content of owner, fingerprinting to identify buyer of content, broadcast monitoring and authentication to determine whether the data is changed from its original form or not.

***Proof of Ownership:*** The important function of watermarking is to remain present in data for proof of ownership. It is enticing to try to use watermarks not just to identify copyright ownership but to actually prove ownership. This is something a textual notice cannot do, because it can be so easily forged. For example, suppose an artist (call her Alice) creates an image and posts it on her website, with the copy right notice c@2001Alice. An adversary (call him Bob) then steals the image, uses an image processing program to replace the copyright notice with "c@2001Bob," and then claims to own the copyright himself. How is the dispute resolved? One way of resolving such a dispute is by use of a central repository. Before putting her image on the Web, Alice could register the image with the Office of Copyrights and Patents by sending a copy to them.

***Broadcast Monitoring:*** This application identifies that when and where works are broadcast by recognizing watermarks embedded in these works. There is variety of technologies to monitor playback of sound recording on broadcast. The DWM is alternative to these technologies due to its reliable automated detection. A single PC based monitoring station can continuously monitor to 16 channels over 24 hours with no human interaction. Resulted monitoring is assembled at central server and is now available to interested one. The system can distinguish between identical versions of songs, which are watermarked for different distribution channel. Such system requires Monitoring infrastructure and watermarks to be present in content. Watermarking video or music is planned by all major entertainment companies possessing closed networks.

***Transaction Tracking:*** In this application of watermarking, the watermark records one or more transactions that have taken place in the history of the copy of a work in which it is embedded. For example, the watermark might record the recipient in each legal sale or distribution of the work. The owner or producer of the work would place a different watermark in each copy. If the work were subsequently misused (leaked to the press or redistributed illegally), the owner could find out who was responsible. In the literature on transaction tracking, the person responsible for misuse of a work is sometimes referred to as a traitor, where as a person who receives the work from as a traitor is a pirate. As this distinction is not meaningful when discussing other applications where piracy is an issue, we do not use this terminology.

***Content Authentication:*** The content authentication is nothing but embedding the signal information in content. This signature then can be checked to verify that it has not been alter. By watermarks, digital signatures can be embedded into the work and any modification to the work can be detected.

***Copy Control:*** In the copy control application, we aim to prevent people from making illegal copies of copyrighted content. The first and strongest line of defence against illegal copying is encryption. By encrypting a work according to a unique key, we can make it unusable to anyone who does not

have that key. The key would then be provided to legitimate users in a manner that is difficult for them to copy or redistribute. For example, many satellite television broadcasts are encrypted. The decryption keys are provided to each paying customer on a "smartcard," which must be inserted in to the customer's television set top box. Anyone trying to watch or record the broadcast without a smart card would see only scrambled video.

***Device Control:*** In the device control application of watermarking for e.g., Digimarc's Media Bridge system embeds a unique identifier into printed and distributed images such as magazine advertisements, packaging, tickets, and soon. After the image is recaptured by a digital camera, the watermark is read by the Media Bridge software on a PC and the identifier is used to direct a web browser to an associated website.

## IV. TECHNIQUES USED FOR DIGITAL WATERMARKING

***Hash Functions as Fragile Watermarks:*** According to Wolfgang and Delp, hash functions can be used as fragile watermarks. One of the methods they have used as watermarks is the block-based hash function (BBHF). The hash is computed on the width and height of the image block. Specifically, $X_b$ is the width of the block and $Y_b$ is the height of the block and $X_b * Y_b$ is the hash function. The hash values of every block of the image are stored. In order to test the sanctity of an image, the stored hash values are compared to the hash values of the image whose sanctity is to be tested. If the hash values do not correspond to each other, then the block which houses the discrepancy is the one that has been altered.

***Variable-Watermark Two-Dimensional Algorithm (VW2D):*** Wolfgang and Delp have developed this algorithm for image authentication. Both the watermark and the watermarked image are used here to authenticate the image. A pseudorandom binary sequence is the watermark and this sequence is superimposed on the original image in blocks. This can be elucidated as follows:

Let WI be the watermarked image, W be the watermark and X be the original image. Then $WI_b$ is a block of the watermarked image, $W_b$ is a block of the watermark and $X_b$ is a block of the original image. The watermarked image is generated as follows:

$$WI = WI_{b1} + WI_{b2} + \ldots + WI_{bn}$$

And each watermarked image block is generated as follows:

$$WI_{bi} = X_{bi} + W_{bi} \quad (\text{where } I = 1 \text{ to } n)$$

Checking to see if a watermark resides in an image (Test) is done as follows:

$$\triangle_{bi} = WI_{bi} . W_{bi} - Test_{bi} . W_{bi}$$

A threshold value can be chosen to authenticate the test image. The threshold is compared with the delta value computed above. The choice of the threshold value can determine the extent of changes that are tolerated to the watermarked image.

***Human Visual System (HVS):*** In order to develop good watermarking algorithms, characteristics of the human visual system have been extensively studied. The nuances of visual perception have given scientists an insight into modeling watermarks that do not interfere with the host image. Wolfgang, Delp and Podilchuk have listed some of the characteristics of the human visual system by the following 3 criteria, as given in Wolfgang et al's paper:

1. Sensitivity to frequency: the HVS is more sensitive to higher frequencies than to lower frequencies.
2. Contrast masking: This refers to how one signal influences the expression of another signal. Presence of two signals in the same frequency enhances this property.

While the above two algorithms have been applied to the spatial domain of the image, watermarking algorithms that tap into various transforms became popular, thanks to their robustness and quality. Some of the transforms that are used for this purpose include the discrete cosine transform (DCT), discrete Fourier transform (DFT) and the wavelet domains. These techniques combined with studies on the human visual system have allowed for the development of good watermarking techniques.

A very popular compression technology for still images is JPEG. Compression in JPEG occurs as follows. The still image to be compressed is passed through a coder, which transforms the image by ripping it into distinct blocks of 8*8 pixels. A DCT is applied on the thus obtained distinct blocks.

*A Semi-Fragile Watermark in the DCT domain –Lin's algorithm:*

Lin et. al. have developed a semi-fragile watermark in the DCT domain.

***Watermark:*** The watermark is given by "pseudo-random zero-mean, unit variance Gaussian distributed numbers".

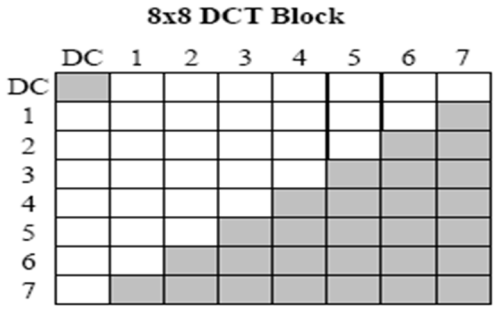


Figure 1: watermarking process using the DCT domain. The clear blocks are marked coefficients while the grey blocks are unmarked coefficients. Figure obtained from ftp://skynet.ecn.purdue.edu/pub/dist/delp/ei00-water/paper.pdf

***Embedding Stage:*** Watermark is embedded in every 8*8 DCT block. Though each block has a different watermark, the watermark is embedded on the same indices of each block. The DC coefficient and some other coefficients including the

high frequency AC coefficients of the block are not marked. The inverse DCT is constructed to produce the watermark W.

WI= O + strength (W),

Where, WI is the watermarked image, O is the original image, and strength is the strength of the watermark.

***Detection Stage:*** Detection is done by comparing blocks with corresponding blocks to localize any changes. A threshold is compared to the test value computed for each of the blocks to figure out if a block has been modified. The algorithm described in Lin's paper is discussed below.

Let B(x,y) be an arbitrary block.

Col-diff (Block(x,y)) = Block(x,y) – Block(x+1,y) for x in { 1,2,…blocksize –1) or 0 if x = blocksize

Row-diff(Block(x,y))= Block(x,y) – Block(x,y+1) for y in { 1,2,…blocksize –1) or 0 if y = blocksize

T is computed as a single matrix obtained by concatenating col-diff anf row-diff of the test image block and water-block is the corresponding matrix for the watermarked image.

T =[Col-diff(T(x,y)) Row-diff(T(x,y))]

W =[Col-diff(W(x,y)) Row-diff(W(x,y))]

Since we need to obtain a dot product, the matrix T and W above are permuted to obtain a vector. The permutation function, F, should be uniform for both the matrices.

F(T) =vector(T)

W(T)=vector(T)

The test statistic, S, can be computed as follows:

S = (T.W) / sqrt((T.T)(W.W))

Comparing the blocks can be done as follows. An appropriate threshold, T, is chosen and compared with the test statistic.

S >= T => block unaltered

S < T => block altered

***The Foundation of Digital Watermarking:*** It should be noted that the reason why digital watermarking is possible is that human vision system (HVS) is not perfect. Digital watermark utilizes the limitation of HVS to make itself invisible, thus avoiding to degrade original digital products, as well being hard to get identified or destroyed.

## VI. MAIN CHARACTERISTICS OF DIGITAL WATERMARKING

***Invisible:*** A watermarking system is of no use if it distorts the cover image to the point of being useless, or even highly distracting. Ideally the watermarked image should look indistinguishable from the original even on the highest quality equipment.

***Robust:*** The watermark should be resistant to distortion introduced during either normal use (unintentional attack), or a deliberate attempt to disable or remove the watermark present (intentional, or malicious attack). Unintentional attacks involve transforms that are commonly applied to images during normal use, such as cropping, resizing, contrast enhancement…etc.

***Unambiguous:*** Retrieval of the watermark should unambiguously identify the owner. Furthermore, the accuracy of owner identification should degrade gracefully in the face of attack.

***Non-perceptibility:*** Watermark cannot be seen by human eye or not be heard by human ear, only be detected through special processing or dedicated circuits.

***Verifiability:*** Watermark should be able to provide full and reliable evidence for the ownership of copyright-protected information products. It can be used to determine whether the object is to be protected and monitor the spread of the data being protected, identify the authenticity, and control illegal copying.

***Security:*** Watermark information owns the unique correct sign to identify, only the authorized users can legally detect, extract and even modify the watermark, and thus be able to achieve the purpose of copyright protection

***Capacity:*** Image watermarking capacity is an evaluation of how much information can be hidden within a digital image. Watermarking capacity is determined by the statistical model used for the host image, by the distortion constraints on the data hider and the attacker, and by the information available to the data hider, to the attacker, and to the decoder.

## VII. CLASSIFICATION OF DIGITAL WATERMARKING

***i) According to the Characteristics:*** Digital watermarking can be divided into robust watermarking and fragile watermarking. Robust watermarking is mainly used to sign copyright information of the digital works, the embedded watermark can resist the common edit processing, image processing and lossy compression, the watermark is not destroyed after some attack and can still be detected to provide certification. Fragile watermarking is mainly used for integrity protection, which must be very sensitive to the changes of signal. We can determine whether the data has been tampered according to the state of fragile watermarking.

***ii)According to the Copyright Protection:*** Digital watermarking can be divided into image watermarking, video watermarking, audio watermarking, and text watermarking and graphic watermarking based on the attached media. Image watermarking refers to adding watermark in still image. Video watermarking adds digital watermark in the video stream to control video applications. Text watermarking means adding watermark to PDF, DOC and other text file to prevent changes of text. Graphic watermarking is embedding watermark to two-dimensional or three-dimensional computer-generated graphics to indicate the copyright.

***iii)According to How Watermark is Detected and Extraction Process:*** Digital watermarking can be divided into visual watermarking and blind watermarking according to the detection process. Visual watermarking needs the original data in the testing course, it has stronger robustness, but its application is limited. Blind watermarking does not need

original data, which has wide application field, but requires a higher watermark technology.

***iv)According to the Ability of Watermark to Resist Attack:*** Fragile watermarks are ready to be destroyed by random image processing methods. The change in watermark is easy to be detected, thus can provide information for image completeness. Robust watermarks are robust under most image processing methods and can be extracted from heavily attacked watermarked image. Thus it is preferred in copyright protection.

***Usefulness of Digital Watermarking:*** The first applications that came to mind were related to copyright protection of digital media. In the past duplicating art the work was quite complicated and required a high level of expertise for the counterfeit to look like the original. However, in the digital world this is not true. Now it is possible for almost anyone to duplicate or manipulate digital data and not lose data quality. Similar to the process when artists creatively signed their paintings with a brush to claim copyrights, artists of today can watermark their work by hiding their name within the image. Hence, the embedded watermark permits identification of the owner of the work. This concept is also applicable to other media such as digital video and audio. Currently the unauthorized distribution of digital audio over the Internet in the MP3 format is a big problem. In this scenario digital watermarking may be useful to set up controlled audio distribution and to provide efficient means for copyright protection, usually in collaboration with international registration bodies. In the field of data security, watermarks may be used for certification, authentication, and conditional access.

***Growth of Digital Watermarking:*** The growth of computer networks has boosted the growth of the information technology sector to a greater extent. There is a trend to move from conventional libraries to digital libraries.

***Challenges in Digital Watermarking:*** The field of digital watermarking has recently seen numerous articles covering novel techniques, theoretical studies, attacks and analysis. We focus on practical challenges for digital watermarking applications. Challenges include design considerations, requirements analysis, and choice of watermarking techniques, speed, robustness and the tradeoffs involved. We describe common attributes of watermarking systems and discuss the challenges in developing real world applications.

## VIII. CONCLUSIONS

This paper starts from some basic knowledge of digital watermarking, includes the classification, techniques, and applications of digital watermarking. There are various kinds of digital watermarking on different medium with different attribution. Then paper gives a brief introduction about digital watermarking algorithm. Algorithm based on spatial domain is important in early days, it is easy to compute but it is also fragile. Most algorithms now are based on transform domain, DWT, DHT, DCT are three commonly used transform domain. Digital watermarking has a widely application, including copyright protection, content protection, locating content online, and so on. Some traditional application and some novel application are introduced in the paper. In conclusion, digital watermarking gives authentication, identification, and integrity to digital signal, and helps the owners can use their digital assets under protection.

**Acknowledgement:** Author Dr S.Madhasia and S.Ahmed is thankful to S.Kapoor, THDC IHET for the generous in the preparation of this manuscript

## REFERENCES

[1] A.H. Ali and M. Ahmad, “Digital Audio Watermarking Based on the Discrete Wavelets Transform and Singular Value Decomposition,” Europe Journal of Science Research, Vol. 39, No. 1, 2010, pp. 6-21.

[2] Bidla P.P., Crengaje S.R., Shelk R.J. “Visible Image Watermarking Based on Texture and Luminance Blocks in DCT Domain – A Review, International Jouranl of Emerging Technology and Advanced Engineering ISSN: 2250-2459, Vol. 2, Issue – 4, 2012.

[3] Chaudhari, B.P.; Gulve, A.K., (2010), “Approaches of Digital Image watermarking using ICA”, Proceedings of ISCET, ISBN: 978-81-910304-0-2.

[4] Cheung, S. C.; Chiu D. K. W. and Ho C., (2008), “The Use of Digital Watermarking for Intelligence Multimedia Document Distribution”, Journal of Theoretical and Applied Electronic Commerce Research ISSN 0718–1876 Electronic Version VOL 3 / ISSUE 3 / DECEMBER 2008 / 103-118.

[5] Jihua, Z., (2004), “Research on Copyright Protection Technology of Digital Image Based on Digital Watermarking”, Doctor Degree thesis. Changsha, Hunan, China: South-Central University for Nationalities.

[6] Jun, J. M.; Lee, B. M.; Kim, K. K. and Won D. H., (2000), “Digital watermarking and practical distribution protocol for digital contents copyright protection”, in Proceedings of the WISA'2000, Seoul, Korea, pp. 251-264.

[7] Katariya S.S., Digital Watermarking Review, International Journal of Engineering & Innovative Technology, Vol. 1, Issue – 2, 2012. ISSN: 2277-3754, pp. 143-153.

[8] M. Thapa and S. Sood, "On Secure Digital Image Watermarking Techniques," *Journal of Information Security*, Vol. 2 No. 4, 2011, pp. 169-184. doi: 10.4236/jis.2011.24017.

[9] Michael, A., (2003), “Techniques and Application of Digital Watermarking”, London: Artech House Publisher.

[10] Podilchuk, C. I.; Delp, E. J., (2001), “Digital watermarking: Algorithms and applications”, Signal processing Magazine.

[11] Qian, L.; Nahrstedt, K., (2005), “Watermarking Schemes and Protocols for Protecting Rightful Ownership and Customer’s Rights”, Journal of Visual Communication and Image Representation, 29(4): pp. 194- 210.

[12] Sharma, R.K., “Practical Challenges for Digital Watermarking Application”, Multimedia Signal Processing, IEEE 4th Workshop, pp. 237-242, 2001.

[13] Su, J.; Hartung, F. and Girod, B., (1998), “Digital watermarking of text, image and video documents, computers and graphics”, Vol. 22, no. 6, pp. 687-695.

[14] Wolfgang, R. W.; Podilchuk, C. I.; Delp, E. J., (1999), "Perceptual Watermarking for Images and Video," Proceedings of the IEEE, (invited paper), Vol. 87, No. 7, pp. 1108-1126.