Review of Dual Watermarking on Digital Image

Etti Mathur
M.Tech Scholar
MACERC, Jaipur

Manish Mathuria
Assistant Professor
MACERC, Jaipur

ABSTRACT

Digital Image Security is still or recent topic of research in computer science engineering. Images are sharing very frequently from one device to another device. Due to this functionality and features it is very complicated situation for all of the application users because users share their personal images publically. A very unsolvable problem is still there is no appropriate method for image security to identify ownership with the image sharing tool over the internet. The digital image watermarking is still appreciable and demandable techniques. Though it is still in research because it has to be utilizing with all the applications those work with images. This research is done to find the best digital watermarking technique to highly secure digital image form the illegal copies. The research work also done to analyze the possibilities of dual watermarking. Various standard research articles were studied and it is found that dual watermarking is possible with some situation. This research work motivates and offers different combinations on digital watermarking techniques in near future for efficient output of watermarking.

Keywords

Digital Image, Digital Watermarking, Discrete cosine transformation (DCT), least significant Bit (LSB),Discrete Wavelet transformation (DWT).

1. INTRODUCTION

Recent years, the digital watermarking technique had been a critical measure for the protection of the multi-media information, and been attached importance to. As a matter of fact, the future development of networked multimedia systems is conditioned by the development of capable methods to protect data owners against illegal copying and rearrangement of the objects put on the network. People invented a technique to secrete the company logo, specific digital identifier and other information into the multimedia files for the sake of identification of ownership. The logical property rights would be protected effectively and the embedded information wouldn't have any effect to the original content. A limiting think about the event of transmission networked services is that authors, publishers `and suppliers of transmission knowledge are `unwilling to permit the distribution of their documents during a networked atmosphere. At that time an invisible watermark message was inserted into a image which is to be transferred such that the invisible message will survive proposed or accidental attacks.
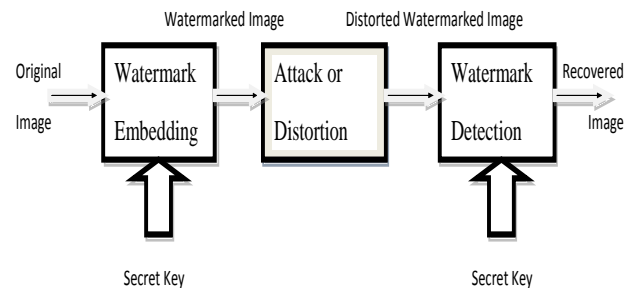

Fig 1. Block Diagram of Watermarking

2. DIGITAL WATERMARKING

Security of data basically means protection of data from unauthorized parties and providing high level security to prevent data modification .The watermark is projected to be permanently embedded into the digital data so that authoritative users can straightforwardly read it[1]. Digital watermarking is a technique which allows a separate to improve secure copyright announcements or additional authentication messages to digital image, audio or video signals and documents [2]. Image watermarking offers the greatest way of image security and certification. The basic theory of the method is that some information could be embedded into the original substance by some unique procedures. A watermarking system is of no substance to anyone if it embedded or distract the cover image to the extent that it being ineffective, or highly distracting to its intended user. In Digital Watermarking, there are two types of Watermarking, Visible and Invisible Watermarking. Digital image watermarking method provides Clarity [3]. Security and Integrity are also two essential requirements of perfect watermarking. A perfect watermarking depends upon the Robustness [4][5].

There are many problems of watermarking-

1. Transparency
2. Security
3. Robustness
4. Imperceptibility
5. Reliability
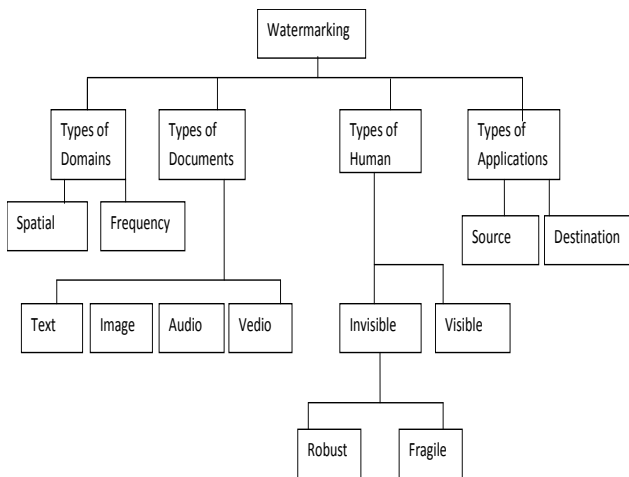
Fig2. Classification of Watermarking

3. DISCRETE COSINE TRANSFORM (DCT)

Discrete cosine transform relies on orthogonal transform that is one in all the most normally used linear transform in digital signal process. It reflects the connection properties of image signal. DCT rule is of moderate complexness, with medium energy consumption and has the great ability to energy compression. Thus, it's wide utilized in digital signal compression like compression and different fields.JPEG compression could be recognized on the idea of the DCT transform. Watermarking rule of JPEG compression normal has greatly increased the power to resist JPEG compression spported watermark. That the DCT transform in watermark technology is incredibly vital [6].
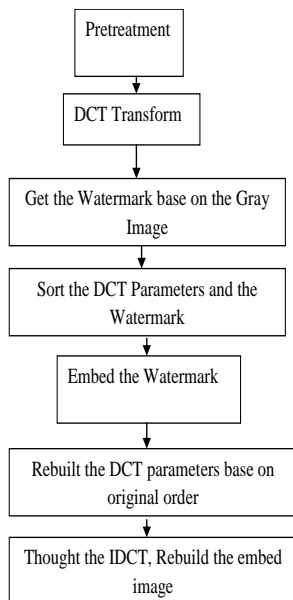

**Fig3. Process of Watermarking using DCT**

4. LEAST SIGNIFICANT BIT (LSB)

The Least significant bit (LSB) is the majority straight-forward technique of watermark embedding and extraction. The most common technique of watermark embedding is to embed the watermark into the smallest amount significant-bits of the cover object.LSB methodology would be to use a pseudo random number generator that confirm the pixels to be

used for embedding watermark primarily based on a given key[7]. Security of the watermark would be increased greatly because the Watermark may now be not is well visible to the hackers or the other inadvertent user. Now a digital image, knowledge is inserted directly into every little bit of image knowledge or the lot of busy areas of an image is calculated therefore on hide such Messages in less noticeable components of an image.
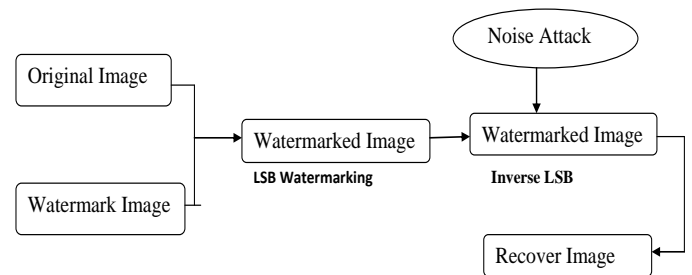
Fig4. LSB Watermarking

5. COMBINATION OF DCT AND LSB
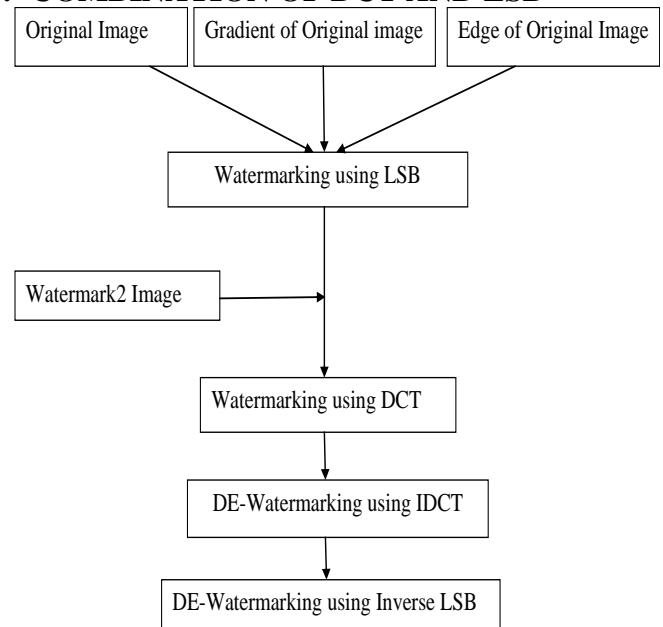
Fig5. Combination of LSB and DCT on Dual Watermarking

Here to show a tendency to used combined approach of LSB-DCT watermarking for multilevel image primarily based knowledge security. In LSB DCT approach author used edge of original image as a watermark image that is calculated by edge detection technique. This watermark is embedded on original image with the help of LSB watermark approach. Once the primary watermarking method is completed author embedded next watermark on the first image with the help of DCT Watermarking.

Advantages:

1. The robustness of the watermarking is dramatically improved
2. It is very complex to erase or damage security information.

3. DCT over LSB does not affect originality of the image.
4. Dual Watermarking hide owner information in very efficient manner such that DCT does not affect the information embedded using LSB.

6. CONCLUSION

However it is very popular to embedded data inside the image using watermarking techniques but the drawback because of the popularity in such that decoding and extraction is very easy and widely available .Many researchers are working to develop such algorithm which requires some complex tactics to decode the embedded information. Digi mark is the company which facilities customer utilize digital technology and to use services in some means of digital watermark technology. It is very new idea to use combination of different watermarking techniques or high security purpose. In the research some selected articles were studied and it is analysis that dual watermarking is possible. Especially DCT is famous for its complexity and LSB is famous for its simplicity. The combination of both DCT and LSB makes best solutions to secure digital documents using digital watermarking. The overall conclusion of this research for achievement that we get the possibilities of dual watermarking specially DCT and LSB and their advantages.

7. REFERENCES

[1] Mauro Barni, Franco Bartolini, Vito Cappellini, lessandro Piva," A DCT-DOMAIN SYSTEM FOR ROBUST IMAGE WATERMARKING", Dipartimento di Ingegneria Elettronica, Universita, di Firenze, via di S. Marta, 3, 50139 Firenze, Italy received 3 February 1997; received in revised form 21 November 1997.

[2] Ranjeet Kumar Singh, Dilip Kumar Shaw and M. Javed Alam," EXPERIMENTAL STUDIES OF LSB WATERMARKING WITH DIFFERENT NOISE", Eleventh International Multi-Conference on Information Processing-2015 (IMCIP-2015).

[3] Puneet Kr Sharma and Rajni." ANALYSIS OF IMAGE WATERMARKING USING LEAST SIGNIFICANT BIT ALGORITHM", International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4, July 2012.

[4] Van Dijk, M. and Willems, F(May 15-16, 2001).: Embedding information in grayscale images. Proc. 22nd Symposium on Information and Communication Theory in the Benelux, pp. 147-154, Enschede, the Netherlands.

[5] A. Nikolaidis, S. Tsekeridou, A. Tefas, V Solachidi(Oct. 2001), "A survey on watermarking application scenarios and related attacks", IEEE international Conference on Image Processing, Vol. 3, pp. 991– 993.

[6] Wu He-Jing," A DCT Domain Image Watermarking Method Based on Matlab", sop transactions on signal processing issn(pRINT): 2377-0538 issn(oNLINE): 2377-0546

[7] Frank Hartung, Martin Kutter(July 1999),"Multimedia Watermarking Techniques", Proceedings of The IEEE, Vol. 87, No. 7, pp. 1085 – 1103.