DIGITAL WATERMARKING USING DCT COEFFICIENT

Happy Makkar[1], Yogesh Juneja[2], Priyanka Garg[3]
Electronics and Telecommunication Engineering ,MDU ,Rohtak
Electronics and Communication Engineering , MDU, Rohtak
Electronics and Communication Engineering , MDU,Rohatk
makkar.happy@yahoo.com
yogeshjunejaer@gmail.com
priyanka0713@gmail.com

Abstract— **The generation & manipulation of digital images is made simple by widely available digital cameras & image processing software .As a consequence , we can no longer take the authenticity of a digital image for granted. So the main concept behind Image authenticity is to protect the trustworthiness of digital images. It verifies the originality of an image by detecting malicious manipulations. It is required to indicate that the data is not a forgery but they should not damage visual quality of the data. The malicious modifications include removal or insertion of certain frames, change of faces of individual, time and background etc. Image authentication techniques protect images from malicious manipulation at every stage of transmission and storage. Reliable image authentication technology must be able to protect an image from the time it was first produced until the final stage of use 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 hiding digital information 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.**

This research paper introduces a watermarking algorithm based on the invisible transform domain using DCT coefficient to improve the value of PSNR.

Keywords— **Digital Image Authentication System (DIAS); Digital Watermarking; Visible Watermarking; Invisible Watermarking; Robust Watermarking; Color Images; Discrete Wavelet Transform (DWT); Haar Wavelet;**

I. INTRODUCTION

The well-known saying is that the photograph doesn't lie" is no longer true due to the availability of powerful image manipulation software. Digital images have been adopted because of their ease of manipulation, processing, and storage and is very old [1].It is almost impossible to distinguish subjectively which images are original, and which have been manipulated. This technical development has decreased the credibility that photography used to achieve. Image authentication techniques have recently gained great attention due to its importance for a large number of multimedia applications. Digital images are increasingly transmitted over non-secure channels such as the Internet. Therefore, military, medical and [2]quality control images must be protected against attempts to manipulate them; such manipulations could tamper the decisions based on these images. Authentication techniques are performed on visual data to indicate that the data is not a forgery; they should not damage visual quality of the video data. Techniques must indicate the malicious modifications include removal or insertion of certain frames, change of faces of individual, time and background etc.

The authentication of documents is still a very critical issue, where it has been researching for century ago. This is a generation of digital data (documents or images). The Government Printing Office (GPO) of U.S. deals with government document to assure the identity. Digital technology has specific power to modify or alter digital data. This is the main reason: the verification of digital documents is not efficient. Image authentication has attained its ground because:

- The easy manipulation property of digital images makes it doubtful [3] when using digital images as evidence in court.
- Image-sharing at social networking makes it prone to be hacked easily.
- For instant, if anyone from or outside the network, access the image and simultaneously upload it to its own account/space. Then, the actual user cannot blame on the other user for ownership of digital content.
- Similarly, for example, any user uploads its important documents as digital images (scan documents) to cloud space at social network.

Unfortunately, if someone can access those documents then he/she may use those documents illegally or fake use. Social Networking is suffering from fakers. Fakers are illegal users, they steel others data and pretends to be just like them by using their digital information. [4]

- Authentication techniques are performed on visual data to indicate that the data is not a forgery.
- The visual quality of the video data should not damage. Only a properly authenticated video data has got the value as legal proof.
- By data authentication it is possible to ensure that data have not been tampered.
- to locate any alteration made on the Image.
- the embedded authentication data be invisible under normal viewing conditions.
- to allow the watermarked image be stored in lossy compression format.
- Two methods have been suggested for achieving the authenticity of digital images having a digital camera sign the image using a digital signature, or embedding a secret code in the image.
- Cryptographic Data authentication
- Watermarking Data authentication[5]

These techniques must indicate the malicious modifications include removal or insertion of certain frames, change of faces of individual, time and background etc. Visual data can be modified using sophisticated processing tools without leaving any visible trace of the modification. So digital or image data have no value as legal proof.

- It is a straight forward way to provide authentication, namely through the joint use of asymmetric key encryption and the digital Hash function.

- To authenticate digital image each camera is assigned a different public or private key pair, with private key hardwired within the cameras. A document encrypted with the private key of any particular camera can be decrypted with its own public key. This property is used to provide center authentication that is to trace back to the true origin of the data.

DRAWBACKS OF CRYPTOGRAPHIC AUTHENTICATION

- Knowledge of key
- Impossible to distinguish between malicious and innocuous modification
- High requirements of video camera
- Delay in transmission
- Protecting privacy is difficult
- Watermarking data authentication is the modern approach to authenticate visual data by embedding a digital watermark signal on the data.
- Digital watermarking is the art and science of embedding copyright information in the original files. The information embedded is called 'watermarks '. Digital watermarks are difficult to remove without noticeably degrading the content.
- A commonly encountered digital watermark is the logo most television channels display on the top of the television screen.

Not only does it advertise the channel but also provides the legal benefit of having a source signature persist during video recording.

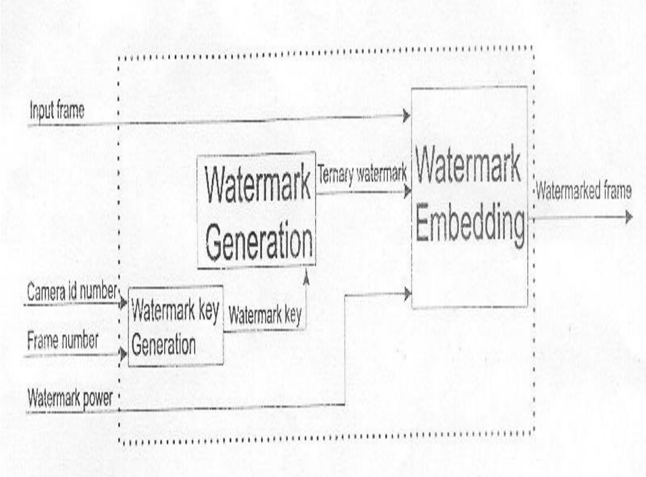

Fig 1 : General Concept of Watermarking

II. TECHNIQUES OF WATERMARKING

According to working domain

- While discussing about the working domain images[6] are represented/stored in spatial domain as well as in transform domain. The transform domain image is represented in terms of its frequencies; whereas, in spatial domain it is represented by pixels.

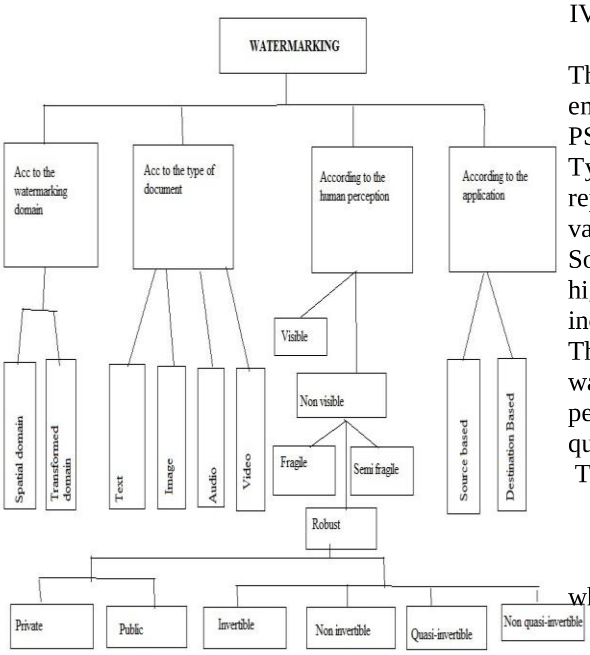

Fig 2: Classification of Watermarking Techniques

III. TRANSFORMED DOMAIN BASED TECHNIQUES

Transform domain means the image is segmented into multiple frequency bands. To transfer an image to its frequency representation, we can use several reversible transforms like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), or Discrete Fourier Transform (DFT). Each of these transforms has its own characteristics and represents the image in different ways. Transformed domain based watermarking schemes are more robust[7,8,9] as compared to simple spatial domain watermarking schemes. Such algorithms are robust against simple image processing operations like low pass filtering, brightness and contrast adjustment, blurring etc. However, they are difficult to implement and are computationally more expensive.

Discrete cosine transform(DCT)[10] turn over the image edge to make the image transformed into the form of even function. It's one of the most common linear transformations in digital signal process technology. Two dimensional discrete cosine transform(2D-DCT) is defined as

$$F(jk) = a(j)a(k)\sum_{m=0}^{N-1}\sum_{n=0}^{N-1} f(mm)\cos\left[\frac{(2m+1)j\Pi}{2N}\right]\cos\left[\frac{(2m+1)j\Pi}{2N}\right]$$

The corresponding inverse transformation (Whether 2D IDCT) is defined as

$$f(mn) = \sum_{m=0}^{N-1}\sum_{n=0}^{N-1} a(j)a(k)F(jk)\cos\left[\frac{(2m+1)j\Pi}{2N}\right]\cos\left[\frac{(2N+1)k\Pi}{2N}\right]$$

IV. IMAGE QUALITY AND SIMILARTY MEASUREMENT

The Peak signal-to-noise ratio (PSNR) is most commonly employed to check quality of image. Higher the value of the PSNR higher is the quality of the image.

Typically, PSNR values which lies between 30 to 50 represents good quality of image. In which higher PSNR value is better.

So, while discussing the authentication of the images we highly concentrate on this factor. The image quality is increased with increasing PSNR.

The *PSNR* is used for evaluating the transparency of watermarking technique for copy protection. Moreover, the peak signal-to-noise ratio (*PSNR*) was used to evaluate the quality of the watermarked image.

The *PSNR* is defined as :

$$\text{PSNR} = 10 \log_{10} \frac{(255)^2}{\text{MSE}}$$

where mean-square error (*MSE*) is defined as

$$\text{MSE} = \frac{\sum (\, I(i) - I'(i)\,)^2}{n}$$

where I (i) and I'(i) are the gray levels of pixels in the host and watermarked images, respectively.

n is the total number of pixels.

The main aim of this research paper is to improve the value of PSNR by implementing an algorithm based in DCT coefficient so here we are using the invisible transform domain based scheme using DCT transform.

V. PROPOSED APPROACH

In this thesis an algorithm based on the DCT coefficient is implemented so as to improve the PSNR value.

Discrete Cosine Transformed (DCT) is used because

- these DCT values contain the low frequency information of watermarking image as these information don't lose or loose little. it means that with DCT we are working with mid band frequency so as to increase the robustness whereas with DWT works on high frequency component of the image.
- The DCT transforms a signal from a spatial representation into a frequency representation. Lower frequency are more obvious in an image than higher frequency so if we transform an image into its frequency component and throw away a lot of higher frequency coefficients, we can reduce the amount of data needed to describe the image without sacrificing too much image quality.
- The discrete cosine transform (DCT) is closely related to the discrete Fourier transform.
- It is a separable linear transformation; that is, the two-dimensional transform is equivalent to a one

dimensional and DCT is performed along a single dimension
followed by a one-dimensional DCT in the other dimension.

We proposed an algorithm with the application of DCT the significant difference part of this algorithm is that here we consider the embedding of random PN sequences into the mid-band components of the DCT -block.

This provides a watermark signal that is quite robust and for most images, transparent.

So, the main task of this work has performed into following steps:

• At the first step, the requirements, techniques and applications of digital watermarking for high-quality images are addressed.

• Second, is to implement the algorithm using the tool (i.e. Mat Lab) for embedding the watermark into original image in DCT domain.

• Then the extraction of watermark will also be implemented. With this, the comparison of original watermark and extracted watermark is also being shown.

• The measurement of quality of an image is also concerned with this work.

The **watermark embedding steps** of this technique are as follows:

Step1: Set gain factor (K) for embedding process.
Step2: Set the DCT block size.
Step3: Perform search to find highly uncorrelated PN sequences (T, F).
Step4: Define the mid-band frequencies of an 8x8 DCT.
Step5: Determine size of original image.
Step6: Determine size of watermark image.
Step7: Reshape the message to a vector.
Step8: Pad the message out to the maximum message size with 1 'so
Step9: Generate shell of watermarked image.
Step10: Generate PN sequences for "1" and "0"
Step11: Process the image in blocks.
Step12: Transform block using DCT.
Step13: If message bit contains zero then embed PN-sequence zero into the mid-band components of the DCT -block.
Step14: Otherwise, embed PN-sequence-one into the mid-band components of DCT-block.
Step15: Transform block back into spatial domain.
Step16: Move on to next block. At end of row move to next row.
Step17: Convert to uint8 and write the watermarked image out to a file.
Step18: Display processing time.
Step19: Display watermarked image.
Step20: Now by repeating the similar steps extract out the watermark from the watermarked image.
Step21: By using the appropriate formulas of PSNR as mentioned into the next subpart of this topic , Calculate the PSNR.
Step 22: Compare the value of PSNR with the value of PSNR calculated by the authors in their paper

VI. SIMULATION RESULTS AND CONCLUSION

In this section the value of PSNR using proposed algorithm is analyzed. Simulation has been done in MATLAB as it provide a friendly image processing toolbox.

The standard 512 x 512-pixels image "Gate" is used as the sample of the test image, as shown in the figure3. The 64 x 64-pixels image "Dmg-l" is used as the sample of the watermark image, as shown in Figure 4. The outcome of the watermarked image is shown in Figure 5.

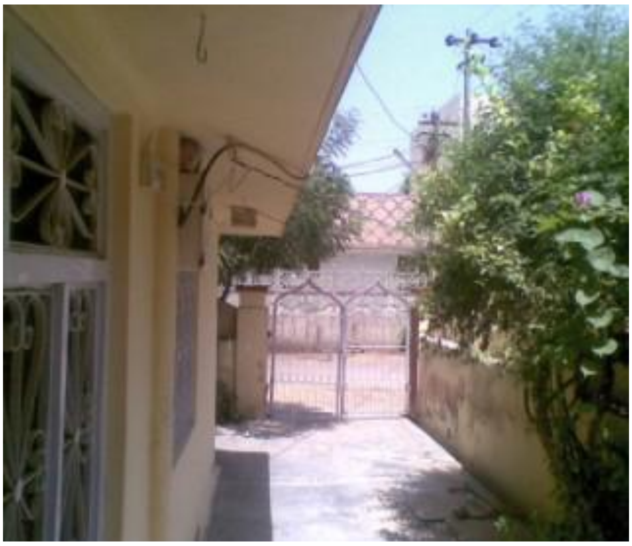

Fig 3 : Original image of Gate.bmp

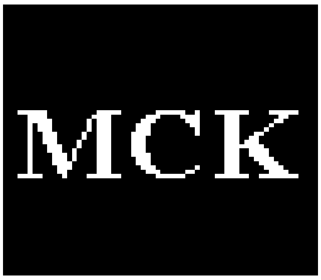

Fig 4: Watermark to be embedded

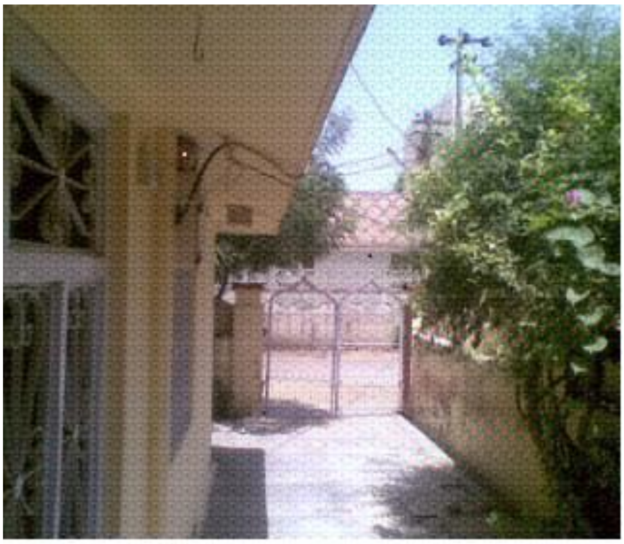

Fig 5: Watermarked image of Gate.bmp

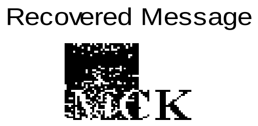

Fig 6 : Extracted watermark

VII. CONCLUSION

Using the proposed algorithm and with the same image we get the value of PSNR = 48.314db which is quite good comparatively

However there are some disadvantages of DCT technique as explained-

- DCT is the basis of many image compression method, for example, for standard JPEG for which DCT is carried out in 8×8 image block existed as main image compression standard for about 10 years. However compression standard for JPEG 2000 accepted quite recently is based on DWT and it commonly provides considerably better quality of decoded image than JPEG. Performance of DCT is almost similar to DWT at lower threshold value but for higher threshold DWT gives better visual image quality than DCT.

VIII. FUTURE SCOPE

- Now-a-days, researchers are focusing on mixing of spatial and transformed domains (i.e. combinations of DFT, DWT and DCT) concepts and also applying more and more mathematical and statistical model, and other interdisciplinary approaches in watermarking: for example use of chaotic theory, fractal image coding etc

- In the wavelet transform domain, high frequency parts represent detailed information of image's edge, contour and texture and so on. Embedding watermarking in these places cannot be easily detected as people are not easily conscious of it. But after processing or attacking, it has poor stability. Most energy of image is centralized in low frequency. Low frequency coefficients are nearly unchanged to common attack so that watermarking information embedded in low frequency coefficients has better robustness.

REFERENCES

[1] Hal Berghel, ”Watermarking Cyberspace”, Communi- cations of the ACM, Nov.1997, Vol.40, No.11, pp.19- 24.

[2] Holliman, M. and Memon, N. (2000) Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes, IEEE Transaction on Image Processing, Vol.9, No.3, Pp.432-441.

[3] Eskicioglu, A. and Delp, E.(2001) An overview of multimedia content protection in consumer electronics devices, Proceedings Signal Processing Image Communication, Vol. 16 Ppp. 681-699.

[4] Image-Based Social Networking websites: www.dailybooth.com and www.pinterest.com

[5] Wang, F., Pan, J. and Jain, L.C. (2009) Digital watermarking techniques, Studies in Computational Intelligence, Springer Berlin / Heidelberg, Vol. 232/2009, Pp. 11-26.

[6] S.P.Mohanty, et al., ”A Dual Watermarking Technique for Images”, Proc. 7th ACM International Multimedia Conference, ACM-MM’99, Part 2, pp. 49-51, Orlando, USA, Oct. 1999.

[7] I.J.Cox et. al., ”Secure Spread Spectrum Watermark- ing of Images, Audio and Video”, Proc IEEE Interna- tional Conf on Image Processing, ICIP-96, Vol.3, pp 243-246, http://www.neci.nj.nec.com/tr/neci tr 95 10.ps

[8] I.J.Cox, et. al., ”A Secure Robust Watermarking for Multimedia”, Proc. of First International Workshop on Information Hiding, Lecture Notes in Comp. Sc., Vol.1174, pp.185-206, Speinger-Verlag, 1996.

[9] I.J.Cox, et al., ”Secure Spread Spectrum Watermark- ing for Multimedia”, IEEE Trans. on Image Process- ing, Vol.6, No.12, Dec 1997, pp.1673-1687.

[10] Tian, J. (2003) Reversible data embedding using a difference expansion, IEEE Transactions on Circuits and Systems for Video Technology, Vol.13, No.8, Pp.890-896.