International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 02 (MAR-APR, 2016)

Commutative Approach for Securing Digital Media

Gyan Singh Ahirwar[1], Kailash Patidar[2]
SSSIST, Sehore, India
[1]gyan98@gmail.com, [2]kailashpatidar123@gmail.com

Abstract:- Multimedia security is very significant concern for the internet technology because of the ease of the replication, distribution and exploitation of the multimedia data. The digital watermarking is a field of information thrashing which hide the crucial data in the original data for protection illegal duplication and distribution of multimedia data. This paper presents a survey on the accessible digital image watermarking techniques. The consequences of various digital image watermarking techniques have been evaluated on the basis of outputs. In the digital watermarking the secret information are entrenched into the original data for protecting the ownership rights of the multimedia data. The image watermarking techniques may split on the basis of domain like spatial domain or transform domain or on the origin of wavelets. The spatial domain techniques straight work on the pixels and the frequency domain works on the transform coefficients of the image. This analysis elaborates the most important methods of spatial domain and transform domain and focus the merits and demerits of these techniques. Digital watermarking is techniques which allocate an individual to add hidden copyright notices or further verification messages to digital audio, video, or image signals and credentials. Watermarking can be prepared by using least significant bit (LSB), singular value decomposition (SVD), Discrete Fourier Transform (DFT), discrete cosine transform (DCT) and Discrete wavelet transform (DWT) techniques. Here this paper discrete cosine transforms (DCT) and Discrete wavelet transform (DWT) are apply for embedding and extraction of watermark. DWT and DCT are evaluating with respect to peak signal to noise ratio (PSNR) at a different threshold values. DWT gives better Image quality then DCT.

Keywords:- Digital watermarking, Spatial domain, Least Significant Bit (LSB), Frequency domain, Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Discrete Fourier Transform (DFT)

I.INTRODUCTION

A digital watermark is a category of marker covertly embedded in a noise-tolerant such as audio, video or image information. It is typically used to distinguish ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in the hidden information should, but does not require to, contain a relation to the transporter signal. Digital watermarks may be used to authenticate the authenticity or integrity of the carrier signal or to show the uniqueness of its owners. It is prominently used for tracing and for authentication. Every digital watermarking technique contains two algorithms: one as the embedding algorithm and other as the recognize algorithm. These two processes are identical for all the type of watermarking techniques. the watermark embedding process in which the watermark is embedded in the cover up image by using the embedding algorithm. Digital Image Watermarking Working Digital Watermarking is a procedure which is used in the digital signal dispensation of embedding hidden information into multimedia data. This information is not generally visible, only dedicated detector or extractor can see and extracts that data. Digital Image Watermarking use digital image for implant the hidden information, after embedding the watermarked image is produce and the watermarked image is further robust against attacks. Figure 3 shows the stages of digital watermarking. Essentially working of digital image watermarking can be alienated in three stages [10]: Embedding phase the embedding stage is the first phase in which the watermark is embedded in the original image by using the embedding algorithm and the secret key. After that the watermarked image is generated. So the watermarked image is transmitted over the network. Distortion/Attack phase in this phase, when the data is transmitted over the network. Either some noise is further with the watermarked image or various attacks are performed on the watermarked image. So, our watermarked data is either modified or shattered. Detection/Retrieval Stage In the detection stage, the watermark is detected or extracted by the devoted detector from the watermarked image by applying some detection algorithm and by using secret key. In accumulation to this, noise is also detected.

II. WATERMARKING TECHNIQUES

An absolute outline of Digital Image watermarking techniques in Spatial as well as transform domain is provided. The study focuses on quality aspect essential for good quality watermarking, Performance evaluation metrics (PSNR and Correlation Factors) and probable attacks. Overview of several methods with spatial and

Transform Domain watermarking is done with detail numerical procedure, their implementations, strengths and weaknesses. The generalized algorithms are accessible for DWT, CDMA stand, DCT-DWT combined approach. The Ridge let Transform is also introduced. Ridge lets are next creation wavelets and they are best preference for line singularities. Ridge lets have high coding performance for 1D wavelet transform. Essentially Ridge let alter is based on radon transform and 1D wavelet transform. It can rotate the picture by procedure in ridge let province. Comparative results of Digital Image Watermarking using LSB, DCT and DWT also exist. The paper recommends DWT foundation techniques for accomplish Robustness in Digital Image Watermarking. The Transform domain watermarking procedures are suggested to achieve robustness. As per ISO Norms, JPEG2000 has replaced DCT by DWT. Hence further researchers are focusing on DWT.

2.1 Discrete Cosine Transform (DCT)

An algorithm of digital watermarking stand on Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) is introduced. According to the characters of human vision, in this algorithm, the data of digital watermarking this have been discrete Cosine transformed, is put into the high frequency band of the image which has been wavelet transformed and after that distils the digital watermarking with the assist of the original image and the watermarking image. The simulation results prove that this algorithm is invisible and has excellent robustness for some common image processing operations. The realized algorithm, called WM2.0, is a watermarking not unsighted algorithm, which embeds watermark signals into high-frequency sub-bands discrete wavelet transform (DWT) coefficients, according to the HVS directives. It makes a pre-processing of the image represent it into component significance of color model hue, saturation, value (HSV) and resizing the value matrix in agreement with the parameters and mathematical base situation of DWT. Wavelet function and DWT level decomposition are fixed, correspondingly, depending on image features and image resize. In the embedding procedure, watermark signal and DWT coefficients to be watermarked are preferred depending on the statistic function values of the image. In the recognition process, original image and watermarked image (expected dissimilar from the output image of the embedding process because of JPEG compression or any attacks) are corresponding comparing statistic function values of a geometric interval of both images; the association between the watermarked DWT coefficients and the watermark signal is calculated according to the Neyman–Pearson statistic condition which determines a recognition threshold minimizing the probability of missing detection to a given possibility of false alarm. WM2.0 is an evolution of a previous algorithm version, WM1.0, described in. In WM1.0 watermark signal and recognition threshold were constant values preferred by means of experimental considerations, thus they were not depending on value image features. The experimentation has been proficient on images, in high and little resolutions, building a real and commercial database. This algorithm has been implemented in Mat lab 6.x using the wavelet and statistic toolbox.

2.2 Discrete Wavelet Transform

The wavelet Transform is basic functions that gratify certain mathematical requirements and using the equivalent function by expanding and shifting to approach the original signal. The wavelet coefficients bring mutually the time and frequency information therefore having excellent local characteristics in Time Domain and Frequency Domain which assist to combine with human vision characteristics. A digital image is decomposed intense on four frequency districts in which there is a low frequency sub band (LL) and three high frequency sub bands (LH, H1, HH). For enhanced diffused and stronger watermark intensities more level decomposition of the image is complete by using wavelet transform. The creative image can be decomposed into frequency districts and sublevel frequency districts data. By doing this the creative image can be decomposed for n level wavelet transformation. The low frequency information image is close to the original image. In this paper we make use of three level wavelet disintegration i.e., low frequency sub band (LL3), Horizontal high frequency sub bands (LH3, LH2, LH1), Vertical high frequency sub band (HL3, HL2, HL1) and Diagonal soaring frequency sub band (HH3, HH2, HH1).

2.3 Applications of watermarking

Digital Watermarks are potentially useful in many applications, including:

1. Ownership assertion. Watermarks can be used for ownership assertion. To assert ownership of an image, Alice can produce a watermarking signal using a secret private key, and then embed it into the original image. She can subsequently make the watermarked image publicly available. Later, when Bob contends the ownership of an image derivative from this public image, Alice can produce the unmarked original image and also demonstrate the presence of her watermark in Bob's image. Since Alice's

International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 02 (MAR-APR, 2016)

creative image is unavailable to Bob, he cannot do the same. For such a scheme to work, the watermark has to carry on image processing operations intended at malicious removal. In addition, the watermark should be include in such a manner that it cannot be fictitious as Alice would not want to be held accountable for an image that she does not own.

2. Fingerprinting. In applications where multimedia content is electronically distributed over network, the substance owner would like to discourage unauthorized duplication and distribution by embedding a distinct watermark (or a fingerprint) in every copy of the data. If, at a later point in time, unauthorized copies of the data are found, then the basis of the copy can be determined by retrieving the fingerprint. In this application the watermark needs to be hidden and must also be invulnerable to deliberate attempts to forge, remove or invalidate. Furthermore, and unlike the ownership declaration application, the watermark should be resistant to collusion. That is, a group of k users with the identical image but containing different fingerprints should not be able to collude and invalidate any fingerprint or create a copy without any fingerprint.

3. Copy prevention or control. Watermarks can also be used for copy prevention and organize. For example, in a closed system where the multimedia content needs special hardware for copying and/or viewing, a digital watermark can be include indicating the number of copies that are permitted. Every time a copy is made the watermark can be modified by the hardware and after point the hardware would not create further copies of the data. An example of such an arrangement is the Digital Versatile Disc (DVD). In fact, a copy protection mechanism that includes digital watermarking at its middle is currently being considered for standardization and second generation DVD players may well include the ability to read watermarks and act based on their presence or absence.

4. Fraud and tamper detection. When multimedia contented is used for legal purposes, medical applications, news reporting, and commercial transactions, it is important to make sure that the content was originated from a specific source and that it had not been changed, influence or falsified. This can be achieved by embedding a watermark in the data. Subsequently, when the photo is checked, the watermark is excavation using a unique key associated with the source, and the integrity of the data is verified through the reliability of the extracted watermark. The watermark can also include information from the original image that can aid in downfall any modification and recovering the original. Clearly a watermark used for authentication purposes should not influence the quality of an image and should be resistant to forgeries. Robustness is not critical as removal of the watermark provide the content inauthentic and hence of no value.

5. ID card security. Information in a passport or ID (e.g., passport number, person's name, etc.) can also be included in the person's photo that appears on the ID. By extracting the embedded information and comparing it to the written text, the ID card can be verified. The inclusion of the watermark provides an additional level of security in this application. For example, if the ID card is stolen and the picture is replaced by a forged copy, the failure in extracting the watermark will invalidate the ID card.

III. DIGITAL IMAGE WATERMARKING WORKING

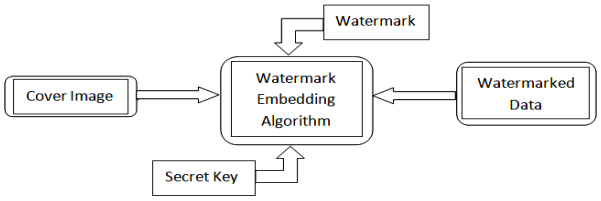

Figure 1Watermark Embedding Process

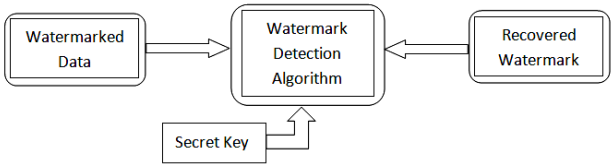

Figure 2 Watermark Detection Process

Digital Watermarking is a technique which is used in the digital signal processing of embedding hidden information into multimedia data. This information is not usually visible, only dedicated detector or extractor can see and extracts that information. Digital Image Watermarking use digital image for embedding the hidden information, after embedding the watermarked image is generated and the watermarked image is more robust against attacks. Basically working of digital image watermarking can be divided in three stages:

A. Embedding Stage: - The embedding stage is the first stage in which the watermark is embedded in the original image by using the embedding algorithm and the secret key. Then the watermarked image is generated. So the watermarked image is transmitted over the network.

International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 02 (MAR-APR, 2016)

B. Distortion/Attack Stage: - In this stage, when the data is transmitted over the network. Either some noise is added with the watermarked image or some attacks are performed on the watermarked image. So, our watermarked data is either modified or destroyed.

C. Detection/Retrieval Stage: - In the detection stage, the watermark is detected or extracted by the dedicated detector from the watermarked image by applying some detection algorithm and by using secret key. In addition to this, noise is also detected.

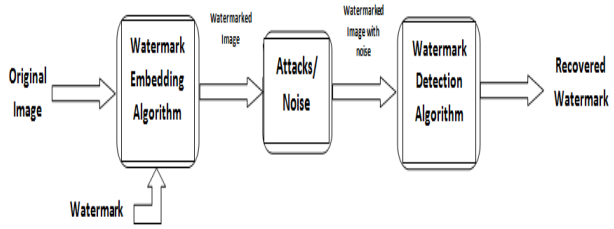

Figure 3 Stages in Digital Image Watermarking

3.1 PSNR Algorithm Description

PSNR is defined as 10*log10 of the ratio of the peak signal energy to the MSE observed between the processed video signal and the original video signal. For the algorithm presented here, the peak signal energy is assumed to be 2552, and the MSE summation is performed over the selected SROI and TROI of the processed video sequence. The algorithm performs a linear fit of the processed image pixels to the corresponding original image pixels for each ST shift that is examined before computing the MSE. This is equivalent to removing gain (contrast) and level offset (brightness) calibration errors in the processed video before performing the PSNR calculation. Computation of PSNR for an (original, processed) video clip pair involves the following steps:

1. Determine the appropriate ST search range for the processed video clip. This involves estimating the x and y spatial uncertainty (in pixels, denoted here as x_uncertand y_uncert) of spatial registration errors that might be present, as well as estimating the t temporal uncertainty (in frames, denoted as t_uncert) of any temporal registration errors that might be present. Since the algorithm will perform an exhaustive search over plus or minus x_uncert, y_uncert, and t_uncert- 4 - shifts of the original video sequence with respect to the processed video sequence, these estimates should be as tight as possible while still including the optimal ST registration.

2. Determine the maximum SROI and TROI that can be used for the processed video clip. If the processed video clip contains truncation of border pixels (i.e., black border), the SROI of the processed video clip should be reduced to eliminate these pixels. If the processed video clip contains transition video frames at the beginning or end of the video clip (perhaps due to prior or following scene content), these frames should be eliminated from the TROI. If necessary, reduce the maximum SROI and TROI to allow for the x_uncert, y_uncert, and t_uncert shifts found in step 1. The final SROI and TROI of the processed video clip that is determined by this step will remain fixed for all PSNR calculations. Since the original video clip will be shifted by a maximum of plus or minus x_uncertand y_uncertpixels and plus or minus t_uncert frames with respect to the processed video clip, one must assure that there are valid original video pixels that align to every processed video pixel within the final SROI and TROI.

3. For each ST shift of the original sequence in step 1, (i.e., shifts in the x, y, and t directions will be denoted here as xS, yS, and tS, respectively), perform a linear fit of the processed pixels to the shifted original pixels. This linear fit is performed for all pixels in the entire ST region encompassed by the processed video SROI and TROI selected in step 2. For a given ST shift, this can be expressed as finding the Gain (xS, yS, tS) and Offset (xS, yS, tS) that minimizes the MSE given by: MSE=1/N∑ ∑ ∑{o(x+xs, y+ys+t+ts) - [gain (xs,ys,ts) * P(x,y,t) + offset(xs,ys,ts)]}(x,y) ESROIT.tETROI, Where three dimensional matrices O and P represent the original and processed video sequences, respectively, the MSE is computed over all x, y, and t that belong to SROI and TROI, and N is the total number of pixels in the three dimensional processed video segment encompassed by SROI and TROI.

4. Compute the MSE in step 3 for all ST shifts within the spatial and temporal uncertainties defined in step 1 (i.e., -x_uncert ≤ xS≤ x_uncert, -y_uncert≤ yS≤ y_uncert, and -t_uncert≤ tS≤ t_uncert) and select the minimum MSE (i.e., MSEmin). This is the MSE that will maximize the PSNR, defined by PSNR=10*$\log_{10}$ (255/MSEmin).

IV EXPERIMENTAL RESULTS

This section elaborates the experimental results of digital image watermarking techniques in MATLAB. Digital image watermarking techniques works in two domains: spatial domain and transform domain. The results of the most important methods of spatial domain as well as transform domain are explained below. In the experimental results, firstly a GUI for showing the results effectively and

International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 02 (MAR-APR, 2016)

implement the most important methods of the spatial domain and transform domain is created. The methods are evaluated on a sample image; either gray scale or RGB image of any size and then watermark image is embedded in the original selected image. After performing LSB method of the spatial domain, the watermarked image is generated. In LSB, the watermark image is embedded into the least significant bits of original image. Mostly used transform domain methods are DCT, DWT and DFT which are used in many fields like compression pattern recognition and in every field of image processing. Then a method of transform domain is applied and transformed image is generated. The GUI of digital image watermarking techniques. (b) The original image which is selected (c) the selected watermark image. (d) Watermarked image after embedding the watermark using LSB method of spatial domain. (e) Shows the DWT transform of original image. The DWT transform the image into multiple resolutions. (f) Shows the DCT transform of the image. The DCT transform the image into different frequency bands. (g) Shows the DFT transform of original image. The DFT transform the image in sine and cosine form.

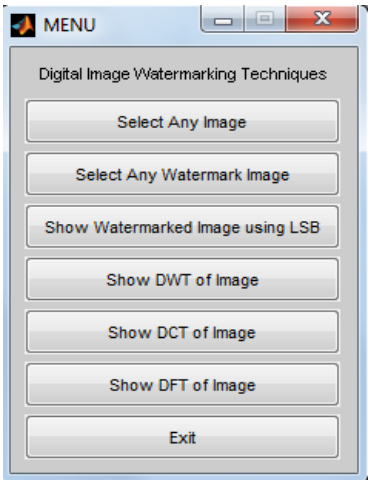

Figure 4 experiment running GUI

Figure 5 Original Image for DIWT

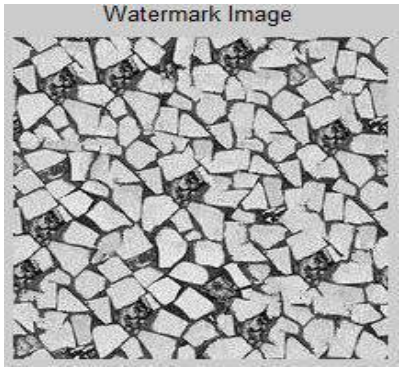

Figure 6 image for water marking

Figure 7 Watermark Image Watermarked Image using LSB

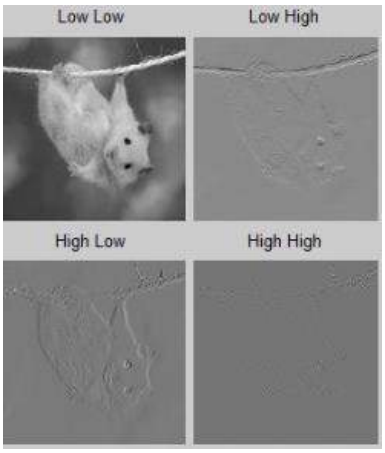

Figure 8 DWT of Original Image

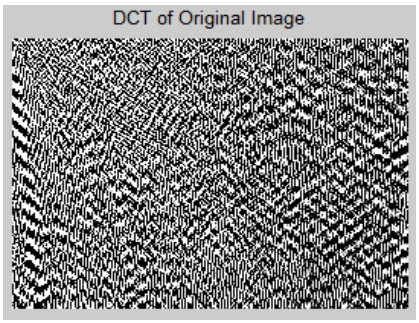

Figure 9 DCT of original image

International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 02 (MAR-APR, 2016)

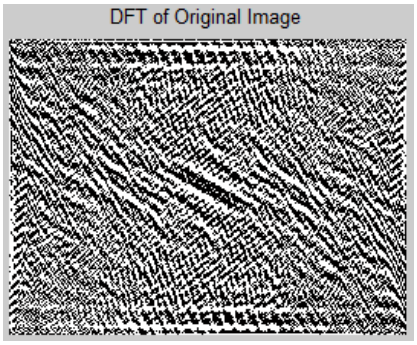

Figure 10 DFT of Original Image

V. CONCLUSION

Digital watermarking is a rapidly evolving area of research and development. We only discussed the key problems in this area and presented some known solutions in this chapter. One key research problem that we still face today is the development of truly robust, transparent and secure watermarking technique for different digital media including images, video and audio. Another key problem is the development of semi-fragile authentication techniques. The solution to this problem will require application of known results and development of new results in the fields of information and coding theory, adaptive signal processing, game theory, statistical decision theory, and cryptography. Although a lot of progress has already been made, there still remain many open issues that need attention before this area becomes mature. This chapter has only provided snapshot of the current state-of-the-art. Digital watermarking is very useful method for providing security to the digital media on the internet technology. In this paper, survey of different techniques based on spatial domain (LSB) and the transform domain (DCT, DWT, and DFT). This survey analyses the limitations and strengths of the watermarking methods. Digital watermarking is still a challenging research field with many interesting problems, like it does not prevent copying or distribution and also cannot survive in every possible attack. One future research pointer is the development of truly robust, transparent and secure watermarking technique for different digital media including images, video and audio.

REFERENCES

[1]. W. Bender D. Gruhl N. Morimoto and A. Lu. Techniques for data hiding. IBM Systems Journal, 35(3-4):313–336, 1996.

[2]. S. Bhattacharjee, "Compression Tolerant Image Authentication", Proceedings, International Conference Image Processing, Chicago, Oct. 1998.

[3]. C. Cachin. An information-theoretic model for steganography Proceedings of 2nd Workshop on information hiding, 1998.

[4]. R. Chandramouli. Data hiding capacity in the presence of an imperfectly known channel process modulation. IEEE Second Workshop on Multimedia Signal Processing, pages 273–278, 1998.

[5]. SPIE Security and Watermarking of Multimedia Contents III, 2001.

[6]. R. Chandramouli. Watermarking capacity in the presence of multiple watermarks and partially known channel. Proc. of SPIE Multimedia Systems and Applications IV, 4518, Aug. 2001.

[7]. B. Chen and G.W. Wornell. Digital watermarking and information embedding using dither.

[8]. B. Chen and G.W. Wornell. Achievable performance of digital watermarking systems. IEEE International Conference on Multimedia Computing and Systems, 1:13–18, 1999.

[9]. B. Chen and G.W. Wornell. An information-theoretic approach to the design of robust digital watermarking systems. IEEE International Conference on Acoustics, Speech, and Signal Processing, 4:2061–2064, 1999.

[10]. A. Cohen and A. Lapidoth. On the Gaussian watermarking game Proc. Intnl. Symposium on Information Theory, page 48, June 2000.

[11]. Digimarc Corporation. http:// www.digimarc.com.