DIGITAL IMAGE WATERMARKING USING DFT ALGORITHM

N. Senthilkumaran and S. Abinaya

[1]Department of Computer Science and Applications, Gandhigram Rural Institute - Deemed University, Gandhigram

ABSTRACT

Image security is a relatively very young and fast growing. Security of data or information is very important now a day in this world. Information security is most important for the business industries. Embedding information so that it cannot be visually perceived. Embedding information in digital data so that it cannot be visually or audibly perceived. In this paper we review some of the digital image watermarking and techniques and then DFT algorithm is also proposed. In this paper we review the robustness and metrics.

KEYWORDS

Watermarking, DFT, Embedding, Robustness

1. INTRODUCTION

Discrete Fourier Transform (DFT) for a finite duration sequence. DFT is a sequence rather than a function of a continuous variable. DFT corresponds to sample, equally spaced in frequency, of the Fourier transform of the signal. The relationship between periodic sequence and finite-length sequences. The Fourier series representation of the periodic sequence corresponds to the DFT of the finite-length sequence. Any function that periodically repeats itself can be expressed as the sum of sines and/or cosines of different frequencies, each multiplied by a different coefficient (Fourier series). Even functions that are not periodic (but whose area under the curve is finite) can be expressed as the integral of sines and/or cosines multiplied by a weighting function (Fourier transform). The frequency domain refers to the plane of the two dimensional discrete Fourier transform of an image. Watermark is a secret message that is embedded into a cover message. Digital watermark is a visible or perfectly invisible. Watermarking process consists two major steps one is location and processing. Location is where to embed watermark. And the process is how to modify the original data to embed watermark. There are two major domain types, spatial and transform domains. Clearly the DFT is only an approximation since it provides only for a finite set of frequencies. But how correct are these discrete values themselves? There are two main types of DFT errors: aliasing and "leakage": This is another manifestation of the phenomenon which we have now encountered several times. If the initial samples are not sufficiently closely spaced to represent high-frequency components present in the underlying function, then the DFT values will be corrupted by aliasing. As before, the solution is either to increase the sampling rate (if possible) or to pre-filter the signal in order to minimize its high frequency spectral content. Recall that the continuous Fourier transform of a periodic waveform requires the integration to be performed over the interval-∞P to +∞P or over an integer number of cycles of the waveform. If we attempt to complete the DFT over a non-integer number of cycles of the input signal, then we might expect the transform to be corrupted in some way.

2. WATERMARKING TECHNIQUES

Watermarking is an embedding process, and it's secured the data. In this watermarking techniques mostly used to business industries. In this techniques are visible, invisible, robust and fragile watermarking. The term **watermark"** was probably **originated from** the German term **"Wassermarke".** Since water is of no important in the creation of the mark, the name is probably given because the marks resemble the effects of the water on paper. Watermarking process is,

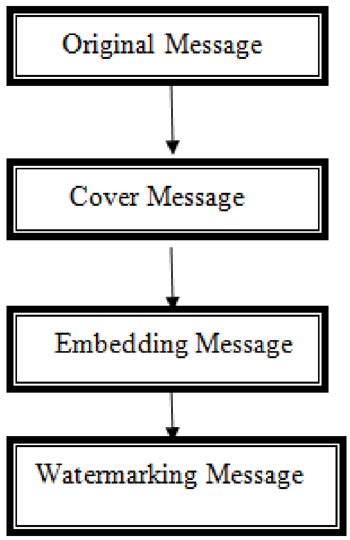
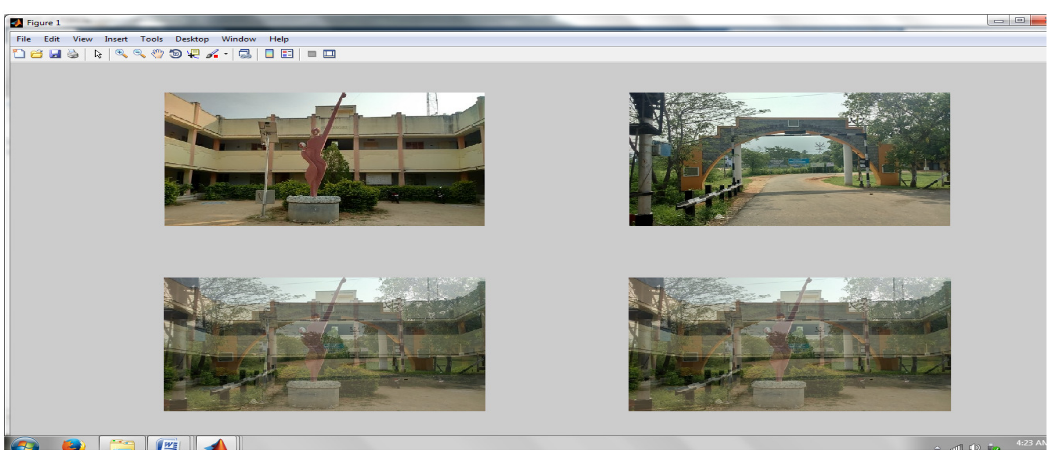


Fig 2.1 Process of watermarking

2.1 Visible Watermark

A visible watermark is immediately perceptible and clearly identifies the cover objects as copyright-protected material, much like the copyright symbols. Logo or seal of the organization which holds the rights to the primary image, it allows the primary image to be viewed, but still visible it clearly as the property of the owning organization. Overlay the watermark in such a way that makes it difficult to remove, if the goal of indicating property rights is to be achieve



2.2. Invisible Watermark

Invisible watermark a copy should be indistinguishable from the original, i.e., the embedding of the watermark should not introduce perceptual distortion of the media object. Since the invisible watermark cannot be detected by the human eye we need some type of extraction algorithm to be able to read the watermark. Invisible watermark do not change the signal to a perceptually great extent, i.e., there are only minor variations in the output signal. The example in the figure shows the invisibly watermarked image [1]

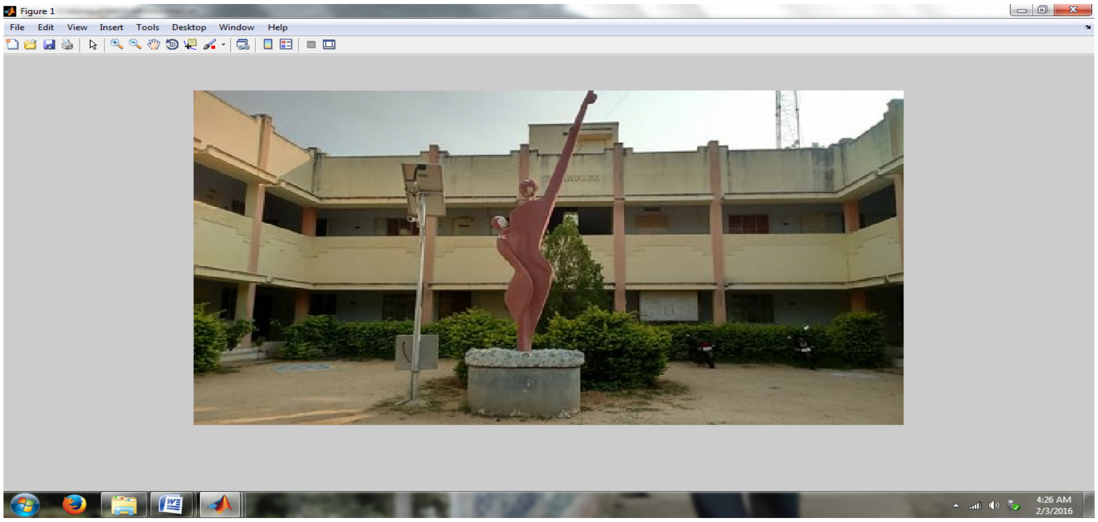


Fig: 2.2 Invisible watermark image

2.3. Robust watermark

A robust watermark must be invariant to possible attacks and remains detectable after attacks are applied. However, it is probably impossible, up to now, for a watermark to

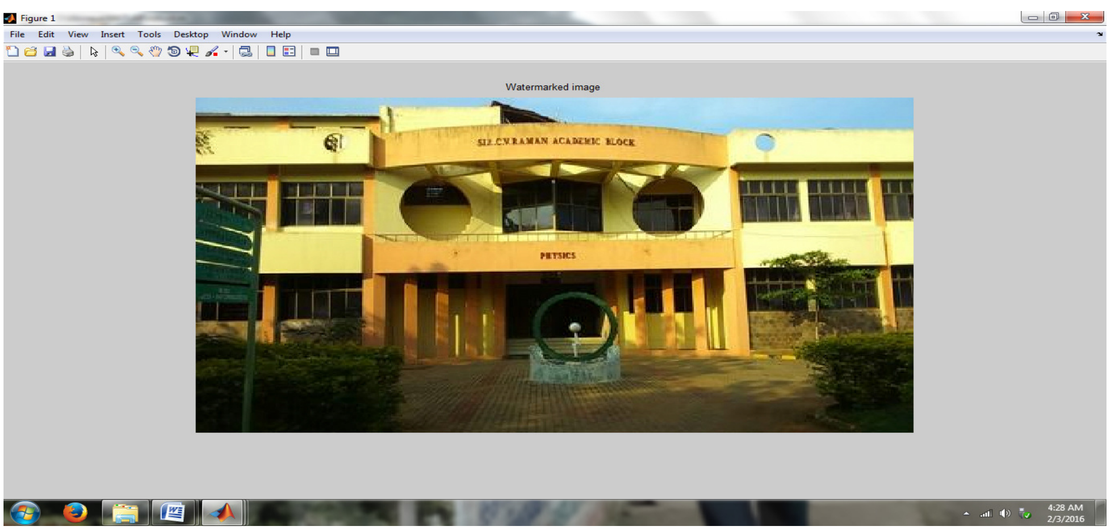


Fig: 2.3 Robust watermark image

resist all kinds of attacks in addition it is unnecessary and extreme [1]. Robust watermark is difficult to remove the original information with embedding information.

2.4. Fragile watermark

A watermark is said to be fragile if the watermark is hidden within the host signal is destroyed as soon as the watermark signal undergoes any manipulation. When fragile watermark is present in a signal, we can infer, with the high probability, that the signal has not been altered [2]. Fragile watermarking authentication has an interesting variety of functionalities including tampering localization and discrimination between malicious and non- malicious manipulations. As to the fragile watermarks for authentication and proof of integrity, the attacker is no longer interested in making the watermarks unreadable. This type of watermark is easy because of its fragility. This host media forgery can be reached by either making undetectable modifications on the Watermarked signal or interesting a fake watermark into a desirable signal[2].

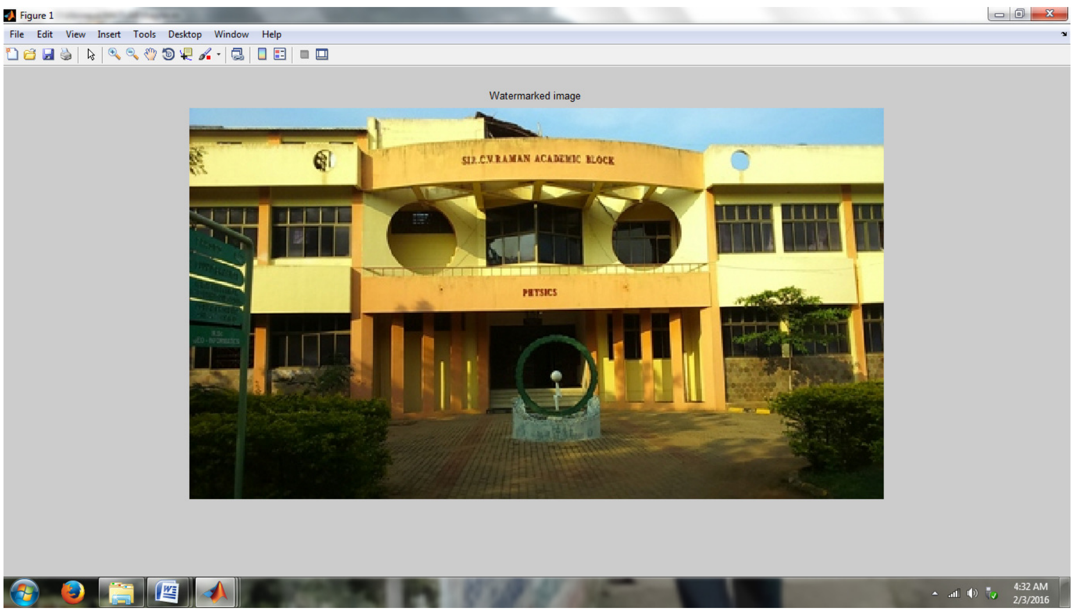


Fig: 2. 4 Fragile watermark image

3. WATERMARKING METRICS

A robust watermarking scheme is often evaluated in four different aspects: payload, distortion, robustness and security [3]. Payload Metrics: The payload metrics is the number of bits of the hidden message conveyed by the watermark. The data hiding capacity of a cover image is calculated as the maximum amount of information that can be embedded and recovered with the low error probability. It is expressed in terms of number of message bits that can be embedded imperceptibility into each pixel of the specific cover image.

$$C=12log2(1+\sigma w2\sigma I2) \text{ bits/pixel(bpp)} \qquad (1)$$

Where, $\sigma w2$ is the variance of watermark which denotes average energy per pixel allowed for the message. $\sigma I2$ is the equivalent Gaussian variance of the image noise [3].

4. RESULT AND DISCUSSION

Images	**Invisible**	**Visible**	**Robust**	**Fragile**
Image1				
Image2				
Image3				
Image4				
Image5				

Fig: 4.1 Resulting images using watermarking techniques

Images	PSNR Value	MSE Value
	29.9611043	66.13
	31.0595575	51.35
	30.5248057	58.08
	28.9627853	83.21

Fig: 4.2 Watermarking image using PSNR and MSE value

5. DISCRETE FOURIER TRANSFORM

The discrete Fourier transform or DFT is the transform that deals with a _nite discrete-time signal and a _nite or discrete number of frequencies.

$$\omega_k = \frac{2\pi}{N}k, \qquad k = 0, 1, \ldots, N-1.$$

For a signal that is time-limited to 0, 1, …, L- 1, the above N ≥ L frequencies contain all the information in the signal. However, it is also useful to see what happens if we throw away all but those N frequencies even for general periodic signals[6].

Discrete-time Fourier transform (DTFT) review

Recall that for a general aperiodic signal x[n], the DTFT and its inverse is,Ref: [5]

$$\mathcal{X}(\omega) = \sum_{n=-\infty}^{\infty} x[n]\, \mathrm{e}^{-\jmath\omega n}, \qquad x[n] = \frac{1}{2\pi}\int_{-\pi}^{\pi} \mathcal{X}(\omega)\, \mathrm{e}^{\jmath\omega n}\, \mathrm{d}\omega .$$

Discrete-time Fourier series (DTFS) review

Recall that for a N-periodic signal x[n] Ref: [5]

$$x[n] = \sum_{k=0}^{N-1} c_k\, \mathrm{e}^{\jmath \frac{2\pi}{N} kn} \quad \text{where} \quad c_k = \frac{1}{N}\sum_{n=0}^{N-1} x[n]\, \mathrm{e}^{-\jmath\frac{2\pi}{N} kn} .$$

Frequency (time) domain: the domain (values of *u*) over which the values of *F*(*u*) range; because *u* determines the frequency of the components of the transform. Frequency (time) component: each of the *M* terms of *F*(*u*). Any function that periodically repeats itself can be expressed as the sum of sines and/or cosines of different frequencies, each multiplied by a different coefficient (Fourier series). Even functions that are not periodic (but whose area under the curve is finite) can be expressed as the integral of sines and/or cosines multiplied by a weighting function (Fourier transform). The frequency domain refers to the plane of the two dimensional discrete Fourier transform of an image. The purpose of the Fourier transform is to represent a signal as a linear combination of sinusoidal signals of various frequencies[7].

5.1 The One-Dimensional Fourier Transform Some Examples

The transform of an infinite train of delta functions spaced by T is an infinite train of delta functions spaced by 1/T.

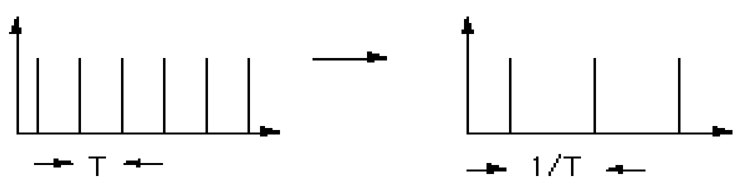
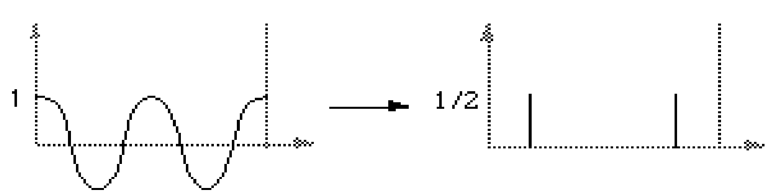
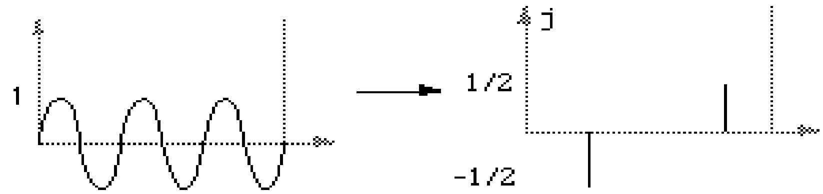


Fig: 5.1.1 One dimensional fourier transform

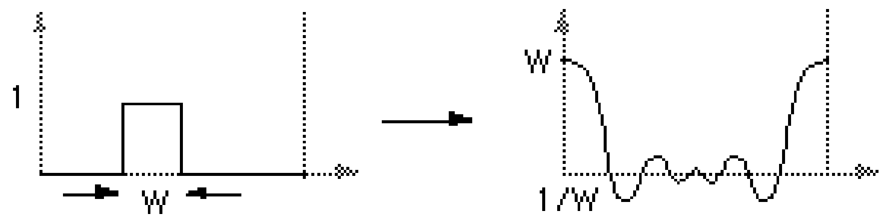
The transform of a cosine function is a positive delta at the appropriate positive and negative frequency [7].



The transform of a sin function is a negative complex delta function at the appropriate positive frequency and a negative complex delta at the appropriate negative frequency[7].



The transform of a square pulse is a sinc function.



The Discrete Fourier Transform (DFT) is the equivalent of the continuous Fourier Transform for signals known only at N instants separated by sample times T _(i.e. a finite sequence of data). Most of the properties of the DTFT have analogous relationships for the DFT. However, our previous definitions of signal properties and operations like symmetries, time-reversal, time-shifts, etc. do not quite work directly for time-limited signals over 0,…, N-1. Time-limited signals are never symmetric in the sense used previously [8].

Fig: 5.1.1 DFT Watermarking Image

Most sequences of real data are much more complicated than the sinusoidal sequences that we have so far considered and so it will not be possible to avoid introducing discontinuities when using a finite number of points from the sequence in order to calculate the DFT. The time taken to evaluate a DFT on a digital computer depends principally on the number of multiplications involved, since these are the slowest operations. With the DFT, this number is directly related to □V(matrix multiplication of a vector), where □ is the length of the transform. For most problems, □ is chosen to beat least 256 in order to get a reasonable approximation for the spectrum of the sequence under consideration – hence computational speed becomes a major consideration. Highly efficient computer algorithms for estimating Discrete Fourier Transforms have been developed since the mid-60. These are known as Fast Fourier Transform (FFT) algorithms and they rely on the fact that the standard DFT involves a lot of redundant calculations:

$$F[n] = \sum_{k=0}^{N-1} f[k] e^{-j\frac{2\pi}{N}nk} \text{ as} F[n] = \sum_{k=0}^{N-1} f[k] W_N^{nk}$$

it is easy to realise that the same values are calculated many times as the computation proceeds. Firstly, the integer product nk repeats for different combinations of k and n values [8].

6. CONCLUSIONS

In this paper proposed to the image watermarking and techniques. In this proposed method is successfully completed the result. In this metrics result is successfully implemented.

ACKNOWLEDGEMENTS

This work was supported by the Gandhigram Rural Institute Deemed University. I thankful to all the personalities for the motivation and encouragements to make this paper work as successful one.

REFERENCES

[1] Yusuf Perwaj, Firoj Perwaj and Asif Perwaj, “An adaptive watermarking techniques for the copyright of digital images and digital image protection”, International journal of multimedia & it’s applications, Vol-4, 2012.
[2] Mahmoud El-Gayyer, “Watermarking Techniques spatial domain rights seminar”
[3] Dae – Jea Cho, “A Study on performance evaluation - Metrics for digital watermarking algorithms”, Advanced Science and Technology letters, Vol-78.
[4] Walid Alakk, Hussain Al-Ahmad and Alavi Kunhu “ A New algorithm for scanned grey PDF files using DWT and hash function”, IEEE journal, 2014.
[5] Anu Bajaj “ Robust and Reversible digital image watermarking technique based on RDWT-DCT-SVD”, IEEE journal, 2014.
[6] J. Fessler, May 27, 2004, 13:14(Student Version)
[7] R. C Gonzalez and R.E Woods,” Digital Image Processing”,2nd Ed, 2002.
[8] Discrete Fourier Transform, www.robots.ox.ac.uk

Authors

S. Abinaya was born in Dindigul-Tamil Nadu at1993. She received her B.Sc. from Madurai Kamaraj University at 2013, dindigul, Tamil Nadu. She received from M.Sc. degree from Mother Teresa Womens University at 2015. Now doing Research in M.Phil Computer Science and Applications in Gandhigram Rural Institute Deemed University, Dindigul, Tamil Nadu .