International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 4 Apr 2022, pp: 1195-1199 www.ijaem.net ISSN: 2395-5252

Development of Image Authentication Application Using Frequency Domain Digital Watermarking System

Amaefule I. A, Agbakwuru A. O., Elei F.O
Department of Computer Science, Faculty of Physical Science Imo State University, Owerri, Imo State-Nigeria
Department of Computer Science, Faculty of Physical Science Imo State University, Owerri, Imo State-Nigeria
Department of Computer Science, Faculty of Physical Science Imo State University, Owerri, Imo State-Nigeria

Submitted: 15-04-2022 Revised: 27-04-2022 Accepted: 30-04-2022

ABSTRACT
Evidently, business and commercial institutions wish to increase their profits, through adoption of multimedia and digital contents. However, the need to protect the ownership of such content when transmitted virtually and other transmission media arises. Digital watermark is a powerful tool to accomplish write protection and digital authenticity. The research is aimed at developing a security system in which pattern of bits are embedded into digital data which does not hinder or degrade the actual data; thus reliability is maintain. The system developed is a web-based application which allows users overlay images in place of text as watermarks unto digital image using Frequency Domain Digital Watermarking methods by employing Discrete Fourier Transformation and its inverse which will reduce the effect of copyright infringement of virtual digital media.

Keywords: Image Authentication, Frequency Domain, Digital Data, Digital Watermark.

I INTRODUCTION

The internet huge acceptance revealed that business potential of presenting multimedia assets over the virtual networks. Ever since business attentions start to utilize virtual networks to provide digital media for gains, they possess a robust attentiveness in safeguarding their right of possession. A potent way out to this difficulty is digital watermarking

Encryption is among the solutions to protect intellectual property right, but then is not sufficient enough because it protect only content during transmission of data from sender to receiver. Data is freely manipulated and distributed and are no longer secured after decryption. Watermarking technique; complement encryption [1]. TV Channels, Certificates, Mark sheets, Bank Currency notes implemented watermarking idea in the imperceptible form.

Hiding of unnoticeable watermark or arrangement or data of bit or insignia into digital documents (video, audio, image, etc.) digital watermarking. [2] Inserting watermark in a manner where standard of the media is not reduced or its perceptible is a watermarking basic principle. Content recovery, authentication and tamper detection are also areas where watermarking can be employed and limited to ownership protection alone.

A Digital Watermarking Features

a. Imperceptibility: The watermark level of noticeability of to the viewer.

b. Robustness: The capability to identify the watermark after common signal processing operations. Watermark must be very strong enough against brightness enhancement, gamma correction attacks so that during signal processing operation watermark would not be removed.

c. Capacity: Amount of data bits a watermark encrypt/encodes in a unit time frame or effort. Watermarks have to contain sufficient details that can denote the distinctiveness of image. It points out the possibility of embedding many watermarks in one domain in parallel.

d. Security: Capability of watermark to withstand against malicious attack.

e. Fidelity: Intuitive likeness linking the actual and watermarked forms of cover work. That means reduction of the standard of actual image through visible distortion of watermarking should be averted. [3].

f. Information Integrity: Embedded watermarking details cannot be changed or detached beyond dependable detection by selected attacks established on a comprehensive knowledge of the embedding technique and the detector. [4]. this indicates that watermark would be arduous to alter or remove without distorting the host communication. [5]. distinctively mark individual image for each buyer is made possible through digital watermarking.

B Simple Watermarking Digital Image Structure

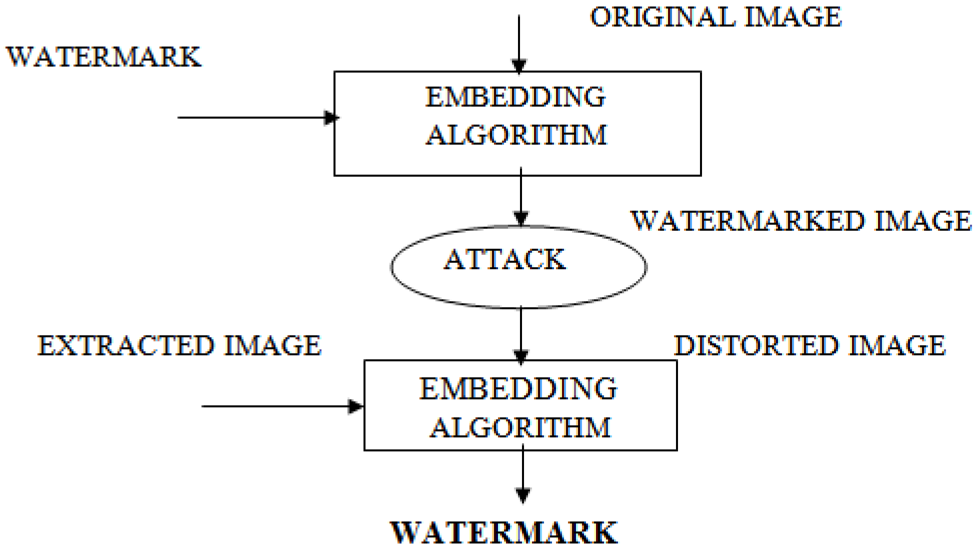

Fig 1: Watermarking Digital Image System

II LITERATURE REVIEW

Signal or pattern that is included in digital image is referred to Digital watermark. Digital Watermark might as well function equally as digital signature used for the duplicates, because this sign or design is existing in every unmodified duplicate of the actual image.

[6]. Researchers have paid countless attention to digital watermarking as a potential mechanism for information security during the past few decades, and has undergone extensive investigation consequently. So far, a diversity of ways and methods have been suggested and put into practice. Two crucial aspects that impact the technique's success are the host values chosen and the method watermark is inserted. They presented a DWT-based channel-wise watermarking system for colored images. Level one DWT is put into each distinct color channel in the algorithm. The end result of the work boasts a robust resistance against numerous attacks like Gaussian noise, JPEG compression, salt and paper noise. The major limitation was; problem in Human vision system and in RGB color images, only blue color is less sensitive to hiding watermark. So, basically why only blue color not others.

[7]. A Robust Multiple Watermarking Method for Information Recovery. They proposed a new technique for multiple watermarking of relational databases in this research, which addresses two important security concerns: ownership identification and information recovery. A secure watermark is implanted using a confidential key recognized solely to the database owner to settle ownership problems. Another watermark includes detailed information on user-specified critical qualities in a manner data which has been interfered with or lost can simply be recovered afterwards. Theoretical research demonstrates that increasing the number of candidate qualities for embedding the watermark raises the chance of successful regeneration of tampered/lost data considerably. They demonstrated that the suggested method is strong enough to excerpt the watermark correctly regardless 100 percent tuple modification or addition, as well as after 98 percent tuple modification or addition. But there major setback was problem of maintaining balance between imperceptibility, robustness and capacity, as increasing one factor adversely affect the other.

[8]. Robust Watermarking for Medical Images Resistant to Geometric Attacks. This study

introduced a novel image watermarking method for medical photos that is resistant to geometric attacks such as scaling, rotation, translation, or these attacks put together. Watermark is incorporated in the image's feature space, which renders it invariant against geometric attacks (rotation, translation, scaling, and combinations of them), and the Arnold transform, that is regarded as disordered scrambling, is put on to the watermarked image to make it more protected. Furthermore, the recommended watermarking structure is sightless as watermark is excerpted without distinguishing the actual image at recipient side. Investigation outcomes established that watermark is strong to counter geometric attacks. They proposed robust watermarking process for medical pictures which is resilient toward Geometric attacks for instance translation, rotation and scaling. The emphasis in this study is on robustness rather than invisibility. Image is first made invariant via statistical moment standardization, before scrambled the watermarked image. However, it has the drawback of not accounting for the invisibility of watermarked images

[9]. A New Digital Watermarking Algorithm Using an LSB and Inverse Bit Combination They presented a new digital watermarking algorithm based on the least significant bit in this study (LSB). Because of its minimal effect on the image, LSB is employed. Prior to implanting the watermark, this novel approach uses LSB to invert the binary values of the watermark text and move the watermark in line with the even or odd number of pixel coordinates of the image. Contingent on the dimension of the watermark text, the suggested approach is adaptable. If the watermark text is extended above ((MxN)/8)-2, the suggested approach will as well implant the watermark text extra in the second LSB. They compare their suggested algorithm to Lee's Peak signal-to-noise ratio algorithm and the 1-LSB approach (PSNR). This novel procedure increased the watermarked image's quality. They also used cropping and noise to assault the watermarked image, and they produced good results. They demonstrated a novel digital watermarking system based on a Least Significant Bit and Inverse Bit combination. They inversed the watermark data and embedded in image by taking different combination of LSB bits. The result was increase in quality of images. However, its limitations are any insignificant change of the amplitude of the signal will change the LSB plane first; therefore any brightness and contrast alteration might destroy all the LSB watermarks.

III DISCRETE FOURIER TRANSFORMATION

In the Frequency Domain, watermarking can be done by using transformations such as the Fast Fourier Transform (FFT), Discrete Cosine Transforms (DCT), Wavelet Transforms, and so on. Because high frequencies are lost when images are compressed or scaled, the Watermark signal is put into lower occurrences, or better still, adjust to occurrences that carry crucial information from the actual image (feature-based schemes). Because watermarks positioned in the frequency domain are scattered across the full spatial image after inverse translation, this technique is less vulnerable to cropping than the spatial method.

FFT is a well-organized procedure for computing Discrete Fourier Transformation (DFT) and its inverse in the suggested system. To compute N points, FFT requires just O (N log N) arithmetic operations. FFT is crucial in an extensive variety of applications, from signal processing to solving partial differential equations to techniques for huge integer multiplication. The system also employs Visible Watermarks that can be seen with the naked eye. These types of watermarks remain simple to see and don't require any mathematical calculations.

This is a transformation that converts a time domain signal to a frequency domain signal. The watermarking is now applied to the modified values rather than the spatial domain values of the image.

Fourier transform in image processing is one of the popular and widely used transforms. Fourier transform is a rendition of an image as an amount of complex exponentials of changing frequencies, phases and magnitudes.

The fundamental Fourier transform turns a signal into an infinite series of sine waves with continuous frequency and amplitude. Most real-world signals, on the other hand, have a finite period and rapid frequency shift (like visuals or music).

Compression, restoration, enhancement and analysis are just a few of the image processing applications where Fourier transform comes in handy.

If f(m, n) is a function of two discrete spatial variables **m** and **n**, then its two-dimensional Fourier transform is defined as follows:

$$\mathbf{F}\,(\omega_1, \omega_2) = \sum_{m=-\infty}^{\infty} \sum_{n=-\infty}^{\infty} \mathbf{f(m,\ n)}\ \mathbf{e}^{-\,j*}\ \mathbf{I}^{m}\ \mathbf{e}^{-\,j*}\ \mathbf{2}^{n}$$

The variables ω**1** and ω**2** are occurrence variables; with radians per sample as their units. The frequency-domain rendition of **F (ω_1, ω2)** is frequently referred to as **f (m, n). F (ω_1, ω2)** is a complex-valued function with period **2**π that is periodic in $\omega_1$and ω_2.

Communication theory establishes that modulating stage is more resistant to noise than modulating amplitude. Furthermore, the stage based watermarks is relatively strong to modifications in image brightness and contrast.

This system presents an efficient transformation method and Image Authentication watermarking. It acts toward the procedure of transforming the actual image using **Fast Fourier Transformation** algorithm.

Since Frequency Domain is used, it takes much time for a hacker to discover the particular frequency that was employed in implanting the watermark; the technique that does not allow intruder to attack the image by JPEG compression, scaling or other methods.

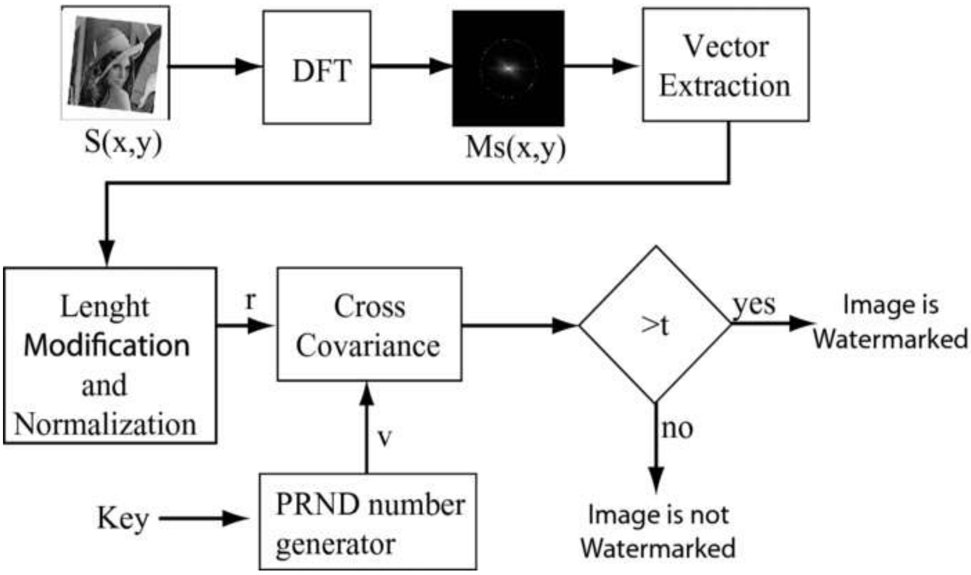

Fig 2: Discrete Fourier Watermarking

IV CONCLUSION

Digital content owners need to properly watermark their data before transmitting over any online source; this ensures that no other duplicate of the data can be discovered elsewhere. This paper presented an online digital watermarking method application that addresses the difficulties encountered by businesses, educational institution and enterprise in securing their digital data. It also fostered good perception of information age and developed efficient and effective watermarking method; it reduces the time, cost, and effort required to secure and safe-guard digital content that requires to be communicated virtually. Acceptance of the method will decrease the effect of copyright violation of digital media over the transmission media and internet.

ACKNOWLEDGMENT

We wish to sincerely thank **TETFUND** for the sponsorship of this research, and also the Vice Chancellor of Imo State University, Owerri for encouraging collaborative research in the institution.

REFERENCES

[1] Mller, M.l., Cox, I.J and Ton kalker," A Review of watermark principal and practices,"published in Digital Signal Processing in Multimedia System,Ed.K.K Parhi and T.Nishitani,Marcell Dekar Inc.,pp.461485,1999.

[2] Kiran and Kanwar Garg (2015) Digital Watermarking: Potential Challenges and Issues. International Journal of Computer Science Engineering and Technology(IJCSET). Vol 5, Issue 3, 48-50

[3] Sen, J., Sen, A.M., and Hemachandran, K., (2012), "An Algorithm for Digital Watermarking of Still Images for Copyright Protection". Indian Journal of Computer Science and Engineering IJCSE

[4] Cox, I.J., Miller, M.L., and Bloom, J.A., (2001), "Digital Watermarking: Principles &Practice". The Morgan Kaufmann

Publishers. ISSN: 2277-3754 ISO 9001:2008 Certified International Journal of Engineering and Innovative Technology (IJEIT) vol.2, Issue 9.

[5] Li, C.T., and Yang, F.M., (2003), "One-dimensional Neighborhood Forming Strategy for Fragile Watermarking". In Journal of Electronic Imaging, vol.12, no.2, pp. 284-291.

[6] Girit, K. J., Peer, M. A., and Nagabhushan, P., (2014), "A Channel Wise Color Image Watermarking Scheme Based on Discrete Wavelet Transformation". In Proceeding of IEEE International Conference on Computing for Sustainable Global Environment transaction, pp. 758-762.

[7] Khanduja, V., Verma, O.P., and Goel, S., (2014), "A Robust Multiple Watermarking Technique for Information Recovery". In IEEE International Advance Computing Conference (IACC), pp. 250-255.

[8] Naseem, M.T., Qureshi, I.M., Raman, A.V., and Muzaffar, M.Z., (2012), "Robust Watermarking for Medical Images Resistant to Geometric Attacks". INMIC, ISSN: 978-4673

[9] Bamatraf, A., Ibrahim, R., and Salleh, M.N., (2011), "A New Digital Watermarking Algorithm Using Combination of LSB and Inverse Bit". Journal of Computing Press, ISSN: 2151-9617, vol.3, no.4.