Hybrid Approach to Digital Watermarking For Secure Communication

Gurkiran Singh
Student, M.Tech CSE,
SUSCET, Tangori, Punjab, India

Abstract: Digital watermarking technology is a frontier research field and it serves an important role in information security. According to the analysis of the definition and basic characteristics of digital watermarking technology, the system model of digital watermarking is given. As an emerging technology, digital watermarking involves the ideas and theories of different subject coverage, such as signal processing, cryptography, probability theory and stochastic theory, network technology, algorithm design, and other techniques. Digital watermarking hides the copyright information into the digital data through certain algorithm. The secret information to be embedded can be some text, author's serial number, company logo, images with some special importance. This secret information is embedded to the digital data (images, audio, and video) to ensure the security, data authentication, identification of owner and copyright protection. The watermark can be hidden in the digital data either visibly or invisibly. The basic principles of digital watermarking technology means that the digital watermark information has a certain significance in the premise does not affect the value of the embedded covertly through a different approach to digital data processing work to become part of the work cannot be separated from the carrier. In the research, we have implemented the DWT and DCT along with proposed hybrid method of watermarking. The proposed hybrid method of watermarking improved the performance, security and efficiency as compared to existing methods. The results are also analyzed on the basis of performance parameters.

Keywords: Steganography; DCT, DWT, LSB, Stego image PSNR, MSE.

I. INTRODUCTION

Digital watermarking is the process of embedding information into a digital signal which may be used to verify its authenticity or the identity of its owners, in the same manner as paper bearing a watermark. For visible identification. In digital watermarking, the signal may be audio, pictures, or video. If the signal is copied, then the information also is carried in the copy. A signal may carry several different watermarks at the same time. Digital watermarking technique is come to know from following three point of views

- **Work** = A specific song, video, picture or specific copy of such.
- **Content** = Set of all possible works.
- **Watermarking** = The practice of imperceptibly altering a work to embed a message about that work.

The watermarking solution promise to protect your images by inserting text information and then tracking the images. Digital watermarking distinguishes digital copies and mark documents with owner’s ID. There are many reasons to embed information in digital content using digital watermarking. The internet boom is one of the reasons. It has become very easy to connect to internet from home computers to obtain or provide various information using World Wide Web (WWW). All information handled on internet is in digital form. Such digital content can be copy such that new file is indistinguishable from original one. Then content can be re-produce in large quantities.

A. Digital watermarking

Digital Watermarking is hidden information inside signal. For watermarking several techniques has been developed. These can be categorized as:

- **Spatial Domain Watermarking**
- **Frequency Domain Watermarking.**

Spatial Domain

Spatial domain watermarking uses block x block watermarking. E.g they embed the watermarks on a randomly selected 8x8 blocks of pixels of the image.

Frequency Domain

To embed a watermark, a frequency transformation is applied to the host data. Then, modifications are made to the transform coefficients. Possible image transformations include discrete Fourier Transform.

B. Applications of Digital Watermarking

Digital watermarking technology for rights management

One of the traditional applications of the watermark is copyright protection. The primary reason for using watermarks is to identify the owner of the content by an invisible hidden “mark” that is imprinted into the image. In many cases, the watermark is used in addition to the content encryption, where the encryption provides the secure distribution method from digital watermarking. The content owners to the receivers, and the watermark offers the content owners the opportunity to trace the contents and detect the unauthorized use or duplications. Without watermarking, there is no way to extend the control of the content owner once the content leaves the protected digital domain and is released to the user. Digital watermark is used to extend the protection and provide the opportunities for the content owners to protect the rights and properties of the electronic distributed contents. The signature of the owner, content ID and usage limitation can be imprinted into the contents, and stay with the contents as far as it travels. This mechanism extends the opportunity of protecting the contents after the release of the contents to the open environment. The major technical requirements for this application are as follows:

- The watermark does not incur visible (or audible) artifacts to the ordinary users.
- The watermark is independent of the data format.
- The information carried by the watermark is robust to content manipulations, compression, and so on.
The watermark can be detected without the unwatermarked original content.

The watermark can be identified by some kind of “keys” that are used to identify large number of individual contents uniquely.

— Digital watermarking technology for authentication and tamper proofing

Another application of digital watermark is contents authentication and tamper proofing. The objective is not to protect the contents from being copied or stolen, but is to provide a method to authenticate the image and assure the integrity of the image. Since low-end digital camera arrived to the consumer market, it rapidly expanded to a number of industrial applications as well, because the use of a digital image is far more cost effective and can also save time and cost for the Developing/Printing/Exposing (DPE) compared to the traditional chemical photos. However, there are some critical issues for some particular applications, where the photos are used as evidence or the material for some kind of business judgment. For instance, automobile insurance companies sometimes use photos of the damaged car sent by the repair shop to estimate the repair cost. A shift to digital photos will save a great amount of time and money for these kinds of processes. However, the digital photos might be altered to exaggerate damage, or even made up from nothing, since the modification of the digital image is getting much easier with some advanced photo-retouching tools be available. This could result in large amounts of extra payment for the insurance company, or more seriously, undermine the credibility of the insurance company itself. A type of digital watermark, called tamper-detect watermark, might resolve this problem, and provide a secure environment for the evidence photos. The way to realize this feature is to embed a layer of the authentication signature into the subject digital image using a digital watermark. This additional layer of watermark is used as a “sensor” to detect the alteration. Our recent implementation can even detect the location of the alteration from the altered image itself. Through a joint study with a major Japanese insurance company, we confirmed the technical feasibility of the technology for the above-mentioned industrial applications. The technical requirements for this application are as follows:

- Invisible to the ordinary users.
- Applicable to compressed image format (most digital cameras use JPEG compatible format).
- Sensitive to content manipulations, compression, and so on.

— Visible reversible watermarking for electronic distribution

Unlike other digital watermarking technologies described above, the visible reversible watermark is visible. It is available as a commercial product. This unique form of watermarking technology by IBM allows the content owners to embed a visible shape or logo mark such as company’s logo on top of the image. The mark is removed (the watermark is reversed) only with the application of an appropriate “decryption” key and watermark remover software. This mark is applied by modifying the Discrete Cosine Transformation (DCT) coefficients of the JPEG compressed image following certain pre-defined rule and visual effect analysis result to make it half transparent, but not totally destructive. The key, with the mark removal program, will be used to remove the mark from the image. The removal of the visible mark may be tied up with the embedding of another invisible mark for the tracking purpose. With this visible watermark on the image, the content becomes self-protective, and content owners can distribute the entire image as a sample to various open media or to the Internet. When a user wants to use a clean copy of the image, all he/she needs to be is to request a “decryption” key and pay some fee for it. This will reduce the security risk and the amount of the data transmission per each buy/sell transaction [5].

II. PREVIOUS WORK

One of the traditional applications of the watermark is copyright protection. The primary reason for using watermarks is to identify the owner of the content by an invisible hidden “mark” that is imprinted into the image. In many cases, the watermark is used in addition to the content encryption, where the encryption provides the secure distribution method from digital watermarking. Considering Chang et al. [14] proposed SVD-based watermarking scheme, which successfully embeds watermarks into images, and its hidden watermarks can resist various attacks. In this paper, we further extend their idea so that the hidden watermarks can be removed to provide authorized users better image quality for later usage after the ownership of purchased images has been verified. To achieve our objective, we modify the embedding strategy, and the extra information required for later restoration is embedded into the least important non-zero coefficients of the S matrices in the image. Experimental results confirm that our scheme not only provides good image quality of watermarked images but also successfully restores images with high restoration quality.

Ahmidi N. et al. [15] discussed focusing on visually meaningful color image watermarks; we construct a new digital watermarking scheme based on the Discrete Cosine transformation. The proposed method uses the sensitivity of human eyes to adaptively embed a watermark in a color image. In addition, to prevent tampering or unauthorized access, a new watermark permutation function is proposed, which causes a structural noise over the extracted watermark. Also, we have proposed a procedure to eliminate this noise to decrease false positives and false negatives in the extracted watermark. The experimental results show that embedding the color watermark adapted to the original image produces the most imperceptible and the most robust watermarked image under geometric and valumetric attacks.

Prerna Singh [16] Digital watermarking techniques have been proposed for copyright protection and authentication of multimedia data. In this paper we are providing one such watermarking scheme for color images. The suggested method presents a watermarking scheme based on a Redundant Discrete Wavelet Transform (RDWT), Discrete Cosine Transform (DCT) and Singular Value Decomposition (SVD) in which two level RDWT is applied on the host image which results in four frequency bands LL2, LH2, HL2 and HH2. As it is found that lower frequency band is less prone to attack, so the singular values of the DCT Transformed coefficients of the LL2 band of the image are being modified using the singular values of the DCT transformed coefficients of the watermark by using scaling factor. Modification of the appropriate sub-band leads to a watermarking scheme which
favorably preserves the quality. The experimental performance of the proposed system is analyzed against different types of attacks, the results show that the proposed RDWT-DCT-SVD method provide the improved imperceptibility, robustness under attacks, provide high data capacity and preserve copyrights. The results demonstrated that the proposed method is more robust to various attacks compared to DWT-DCT-SVD based method.

Christian Rey et al. [17] Digital image manipulation software is now readily available on personal computers. It is therefore very simple to tamper with any image and make it available to others. Insuring digital image integrity has therefore become a major issue. Watermarking has become a popular technique for copyright enforcement and image authentication. The aim of this paper is to present an overview of emerging techniques for detecting whether image tampering has taken place. Compared to the techniques and protocols for security usually employed to perform this task, the majority of the proposed methods based on watermarking, place a particular emphasis on the notion of content authentication rather than strict integrity. In this paper, we introduce the notion of image content authentication and the features required to design an effective authentication scheme. We present some algorithms, and introduce frequently used key techniques.

AnkitaDurge et al. [18] Digital watermarking is used to hide the information inside a signal, which cannot be easily extracted by the third party. Its widely used application is copyright protection of digital information. It is different from the encryption in the sense that it allows the user to access, view and interpret the signal but protect the ownership of the content. One of the current research areas is to protect digital watermark inside the information so that ownership of the information cannot be claimed by third party. With a lot of information available on various search engines, to protect the ownership of information is a crucial area of research. In recent year, several digital watermarking techniques are presented based on discrete cosine transform (DCT), discrete wavelets transform (DWT) and discrete fourier transforms (DFT). In this paper, we proposed an algorithm for digital image watermarking technique based on singular value decomposition; both of the L and U components are explored for watermarking algorithm. This technique refers to the watermark embedding procedure and watermark extracting procedure. Digital image watermarking techniques for copyright protection is robust. The experimental results prove that the quality of the watermarked image is good and that there is strong resistant against many attacks. The image watermarking techniques help to achieve artificial intelligence. Digital image watermarking is the most effective solution in this area and its use to protect the information is increasingly exponentially day by day.

ShaikhAjjiAmirsab et al. [19] Digital watermark has been presently utilized as a possible solution for intellectual property rights protection. It is a technique for labeling multimedia data, including digital images, text documents, video and audio clips, by hiding secret information in the data. This embedded hidden information is unperceivable so the watermarked data appear identical to the original non-watermarked data. Moreover, this hidden information can neither be removed nor decoded without the required secret keys or algorithms. The current classical algorithm contains spatial domain algorithm and transformed domain algorithm. With the spatial domain algorithm, the embedding and the distilling of watermarking are finished in spatial domain, by emending directly or comparing the gray-level value or colour value. The classical spatial domain algorithms including several ways as follow: the least significant bit (LSB), Patchwork method with streak block map decoding, the method based on district intersecting and so on. Then the main current transformed domain algorithms are spread spectrum, DCT transformation method and DWT transform method. against most common attacks. Analysis and experimental results show higher performance of the proposed method in comparison with the DWT-SVD method.

Ahmidi N. et al. [15] discussed focusing on visually meaningful color image watermarks; we construct a new digital watermarking scheme based on the Discrete Cosine transformation. The proposed method uses the sensitivity of human eyes to adaptively embed a watermark in a color image. In addition, to prevent tampering or unauthorized access, a new watermark permutation function is proposed, which causes a structural noise over the extracted watermark. Also, we have proposed a procedure to eliminate this noise to decrease false positives and false negatives in the extracted watermark. The experimental results show that embedding the color watermark adapted to the original image produces the most imperceptible and the most robust watermarked image under geometric and volumetric attacks.

III. PROBLEM FORMULATION

Digital watermarking technology is a frontier research field and it serves an important role in information security. According to the analysis of the definition and basic characteristics of digital watermarking technology, the system model of digital watermarking is given. The system consists of two modules which are watermark embedding module and watermark detection and extraction module. Digital watermarking is used to hide the information inside a signal, which cannot be easily extracted by the third party. Its widely used application is copyright protection of digital information. It is different from the encryption in the sense that it allows the user to access, view and interpret the signal but protect the ownership of the content. One of the current research areas is to protect digital watermark inside the information so that ownership of the information cannot be claimed by third party. With a lot of information available on various search engines, to protect the ownership of information is a crucial area of research. In the research, new hybrid digital image watermarking approach is proposing and from the results will be obtained on the basis of performance metrics. The ultimate objective of the research is to prove that the propose method of watermarking is efficient based on the quality of the watermarked images and recover watermark after different attacks. The propose method will also provides better image quality and better watermark extraction than the existing methods.

IV. RESEARCH OBJECTIVES

A Watermark is a form, image or text that is impressed on to paper, which provide evidence of its authenticity.
Digital Watermarking is an extension of this concept in the digital world. The objectives of the research work are:

• To study and analyze the existing techniques for watermarking.

• To apply the DWT and DCT to watermark image and decompose it into sub bands.

• To apply the propose hybrid method (LSB + DFT) to watermark image for efficiency and to improve the security.

• To compare and analyze the existing and propose techniques on the bases of performance metrics.

V. RESULT & DISCUSSION

Watermarking is the part of practice of covering a message, file, image within another image, message etc. The word Watermarking is of Greek origin and means "covered writing" or "concealed writing". It combines the Greek words steganos meaning "covered or protected", and graphei meaning "writing". In the present electronic communication scenario, data security is one of the major challenges. After the World War II, the need for a secure and robust communication between the communicating entities has increased due to the fear of terrorism. The publishers of digital audio and video are worried of their works being corrupted by illegal copying or redistribution, hence it is of primary importance to protect information. Cryptography is the method to hide secret data by scrambling so that it is unreadable, however it does not assure security and robustness as the hacker can obviously guess that there is a confidential message passing on from the source to the destination. Watermarking is concealed writing and is the scientific approach of inserting the secret data within a cover media such that the unauthorized viewers do not get an idea of any information hidden in it. Watermarking is an alternative to cryptography in which the secret data is embedded into the carrier in such way that only carrier is visible which is sent from transmitter to receiver without scrambling. The combination of Cryptography and Watermarking provide high level security to the secret information.

Implementation Steps
1. Uploading of image sample
2. Implementation of Different Techniques (DWT, DCT and LSB + DFT)
3. Uploading watermark image
4. Extraction of watermarked image
5. Performance Evaluation in terms of mean square error rate.

Below are the snapshots for implementation. The developed system is simulated using MATLAB 2015.

a. The above figure shows the graphical user interface panel in which user interface controls are given which deals with the panels, pushbuttons, static text. The above figure consists of the pushbuttons for each category buttons through which the operations are performed will able to achieve the system performance.
The above figure shows the panel having hybrid approach using hybridization of low significant bit and discrete Fourier transform. The LSB is the lowermost significant bit in the matrix of the image pixel. The LSB grounded image watermarking embeds the image which is to be watermarked in the least significant bits of pixel values of the cover image. It is one of the robust techniques in image hiding. Then the output matrix is fed as the input on which discrete Fourier transform will perform operations. Then DFT changes a finite order of equally-spaced pixel samples into an equal sequence of same length which is a frequency in a complex form and the performance is evaluated using mean square error rate and we can estimate the proposed approach is able to achieve less error rate than the DWT and DCT.

The above figure shows the DWT image using low pass approximation and the watermarked image and also shows the mean square error rate which must below for the high suitability of the system that how much your system is well efficient to perform watermarking process using DWT.

The above figure shows the discrete cosine transform. The whole execution process is same; the only difference is in the DWT process. In place of DWT we have used discrete cosine transform. The DCT is similar to the discrete Fourier transform which transforms an image from the spatial domain part to the frequency domain part. We can see the performance in terms of mean square error rate which shows the how much our system is taking total error rates traditional techniques which is discrete wavelet transform and discrete cosine transform.

The above figure shows the mean square error rate graph using DWT and is tested on different sample of the image. From the above graph we found that the first sample is achieving less mean square error rate than test samples which is 0.001
VI. OUTPUT TABLES AND GRAPHS

Table 1 shows the comparison table in terms of mean square error rate on different test sample images. The table shows clearly that our proposed approach is able to achieve less mean square error rate than the first sample is achieving less mean square error rate than test samples which is 0.001

Table 1: Result Comparison

<table>
<thead>
<tr>
<th>Test Samples</th>
<th>DWT</th>
<th>DCT</th>
<th>Hybrid (LSB+DFT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.001</td>
<td>0.98</td>
<td>4.78×10^{-8}</td>
</tr>
<tr>
<td>2</td>
<td>0.0016</td>
<td>0.99</td>
<td>8.13×10^{-8}</td>
</tr>
<tr>
<td>3</td>
<td>0.0013</td>
<td>0.89</td>
<td>7.23×10^{-8}</td>
</tr>
</tbody>
</table>

VII. CONCLUSION AND FUTURE WORK

Digital watermarking has become a promising research area to face the challenges created by the rapid growth in distribution of digital content over the internet. To prevent misuse of this data Digital watermarking techniques are very useful in which a Secret message called as a watermark can be a logo or label is embedded into multimedia data imperceptibly which would be then used for various applications like copyright protection, authentication, and tamper detection etc. In the future, we will explore the new techniques for digital image watermarking, and also will use other parameters for measurement.

A. Future work

Digital watermarking used as covert communication adds an extra level of security compared to cryptography. In cryptography, the data is encrypted and can only be decrypted using a secret key. However, the attacker is aware of the existence of such data and can be certain that with enough time, he can decrypt the data, where as in digital watermarking, the attacker can never be certain that secret information is being transmitted.

Another advantage of digital watermarks is that it continues to exist even after the receiver obtains the information. Digital watermarking combined with cryptography is highly desired. In the research, we have studied the existing techniques of watermarking, and we implemented the DWT and DCT along with proposed techniques for watermarking. The proposed method of watermarking improved the security and efficiency as compared to existing methods of watermarking. The results are analyzed for proposed method on the basis of performance parameters.

REFERENCES


