Volume: 3 Issue: V Month of publication: May 2015

DOI:

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

An Efficient Fast Hadamard Transform Oriented Digital Image-In-Image Watermarking

Bendalam Vijay[1], Jallu Swathi[2]
[1]Assistant Professor,Department Of CSE, [2]Assistant Professor, Department Of Ece
[1,2]Aitam, Tekkali Srikakulam, Andhrapradesh, India

Abstract: The World Wide Web is, in many respects, a world without barriers. Its openness is highly appealing, if not downright noble. Unfortunately people can take advantage of this electronic latitude to unlawfully take what is not theirs. Efforts aimed at protecting intellectual property are limited to crop up gateways that show lengthy legal documents establish ownership; it does not provide enforcement of tracking stolen intellectual property in the digital world. Digital watermarking is one of the proposed solutions for protection of intellectual property. Digital watermarks are designed to be persistence in viewing, printing or subsequent retransmission. Thus, Digital watermarking does not prevent copying but it deters illegal copying by providing a means for establishing the original ownership of a redistributed copy. A Digital watermark is a digital signal inserted into a digital image. Since this signal is present in each unaltered copy of the original image, the digital watermark may also serve as digital signature for the copies. This subject has been quite exhaustively researched and several techniques have been established for protecting copyright for still images, audio and video files. In this paper, we propose an efficient Fast Hadamard Transform oriented Digital Image-In-Image Watermarking for the copyright protection. This algorithm can embed or hide an entire image or pattern as a watermark into the original image. The performance of the proposed technique is better compared to other techniques like Discrete Cosine Transforms, Discrete Wavelet Transforms. It can extract better-quality watermarks and it takes little time to embed and extract the watermark.

I. INTRODUCTION

The unauthorized copying of many types of media has been a subject of concern for several years. In the past these copies have been obvious due to depreciation of quality which occurs when using analog techniques. Nowadays, with the home computer being very popular and widespread, digital copying is easy and hundred percentage facsimiles of images, video, audio and text can be produced quickly and cost effectively. Distribution of these files occurs rapidly due to the internet being available in most homes. The World Wide Web is responsible for a vast increase in pirated media due to its availability and speed of distribution. Files can be manipulated or modified easily with wide ranges of software and people often claim that these modified files are theirs when in fact they were originally produced by somebody else[10].

To stop these perfect digital copies and modified files several methods such as copy protection and file encryption have been tried and until recently, have failed. These old techniques suffer from major drawbacks. Once an encrypted file has been decoded successfully, it can be copied as many times as for redistribution with no encryption. Thus, there is a strong need for techniques to protect the copyright of content owners. Cryptography and digital watermarking are two complementary techniques to protect digital content [6].

Cryptography is the processing of information into an encrypted form for the purpose of secure transmission. Before delivery, the digital content is encrypted by the owner by using a secret key. A corresponding decryption key is provided only to a legitimate receiver. The encrypted content is then transmitted via Internet or other public channels, and it will be meaningless to pirate without the decryption key. At the receiving end, the receiver decrypts the information by using secret key which is shared by both deliver and receiving end. However, once the encrypted content is decrypted, it has no protection anymore. For example, an adversary can obtain the decryption key by purchasing a legal copy of the media but then redistribute the decrypted copies of the original [23].

In response to these challenges, Digital watermarking techniques have been proposed to protect the digital content even after it is decrypted. In digital watermarking, a watermark is embedded into a covertext, resulting in a watermarked signal called stegotext which has no visible difference from the covertext. In a successful watermarking system, watermarks should be embedded in such a way that the watermarked signals are robust to certain distortion caused by either standard data processing in a friendly environment or malicious attacks in an unfriendly environment. In other words, watermarks still can be recovered from the attacked watermarked signal generated by an attacker if the attack is not too much [10, 5].

A. Digital Watermarking History and Terminology

1) History: The idea of communicating secretly is as old as communication itself. Steganographic methods made their record debut a few centuries later in several tales by Herodotus, the father of history. Kautilya's Arthasastra, Lalita Visastra are few famous examples of the Indian literature in which secret writing or steganography have been used. Few other examples of steganography can be found. An important technique was the use of sympathetic inks. Ovid in his Art of Love suggests using milk to write invisibly. Later, chemically affected sympathetic inks were developed. This was used in World Wars 1 and 2. The origin of steganography is biological and physiological. The term steganography came into use in 1500's after the appearance of Trithemius book on the subject Steganographia. In World War 1, for example, German spies used fake orders for cigars to represent various types of British warships-cruisers and destroyers[9].

2) Terminology: Because most of the techniques used to hide or embed data in media share similar principle and basic ideas, this section will gives some definitions, to avoid confusion, to clarify and make the difference between these different techniques. The various information hiding techniques can be classified as given in Fig 1.1

Steganography stands for the art, science, study, work of communicating in a way which hides a secret message in the main information. Steganography methods rely generally on the assumption that the existence of the covert data is unknown to unauthorized parties and are mainly used in secret point-to-point communication between trusting parties. In general the hidden data does not resist manipulation and thus cannot be recovered.

Watermarking as opposed to steganography, in an ideal world can resist to attacks. Thus, even if the existence of the hidden information is known, it should be difficult for an attacker to remove the embedded watermark, even if the algorithmic principle is known.

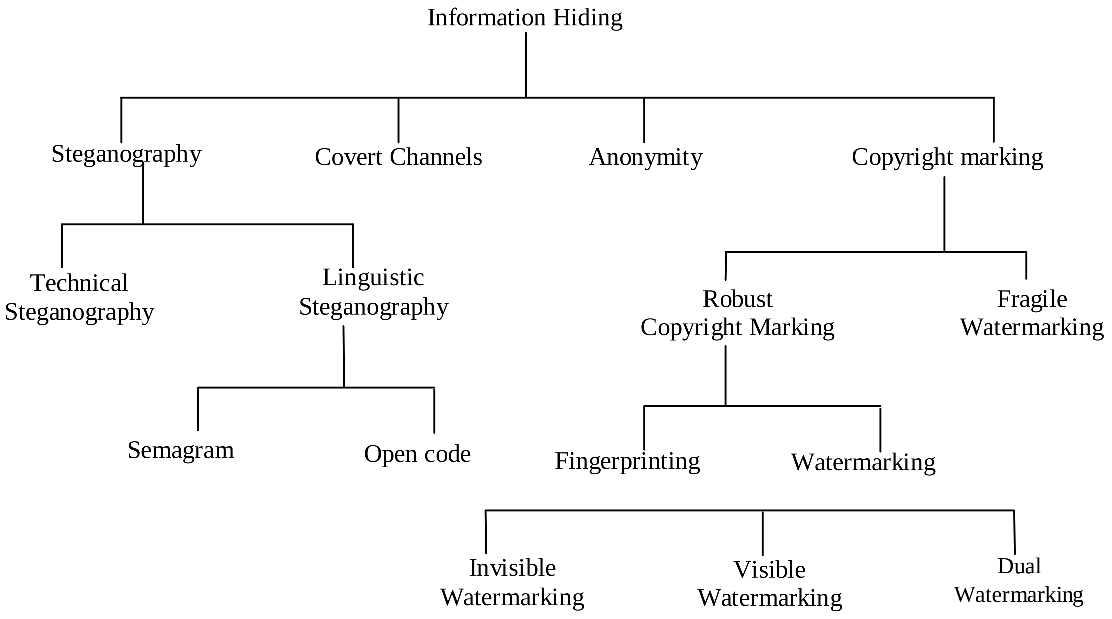


Figure 1.1. Information Hiding Techniques

Data hiding and Data embedding are used in varying context, but they do typically denote either steganography or applications "between" steganography and watermarking applications where the existence of the embedded data are publicly known, but do not need to be protected.

Fingerprinting and labeling are terms that denote special applications of watermarking. They relate to copyright protection applications where information about originator and recipient of digital data is embedded as watermarks. The individual watermarks, which are unique codes out of a series of codes, are called "fingerprints" or "labels."

Bit-stream watermarking is sometimes used for data hiding or watermarking of compressed data, for example, compressed video.

Visible watermarks as the name says, are visual patterns, like logos, which are inserted into or overlaid on images, very similar to visible paper watermarks.

Copy protection attempts to find ways, which limits the access to copyrighted material and/or inhibit the copy process itself.

Copyright protection inserts copyright information into the digital object without the loss of quality. Whenever the copyright of a digital object is in question, this information is extracted to identify the rightful owner. It is also possible to encode the identity of the original buyer along with the identity of the copyright holder, which allows tracing of any unauthorized copies.

B. Research Problems and Motivations

A major research problem on digital watermarking is to determine best tradeoffs among the distortion between the covertext and stegotext, the distortion between the stegotext and forgery, the watermark embedding rate, the compression rate and the robustness of the stegotext. Along this direction, some information theoretic results, such as watermarking capacities and watermarking error exponents, have been determined. Watermarking is not a new phenomenon. For nearly one thousand years, watermarks on paper have been used to identify a particular brand (in the case of publishers) and to discourage counterfeiting (in the case of stamps and currency). In the contemporary era, proving authenticity is becoming increasingly important as more of the world's information is stored as readily transferable bits. Digital watermarking is a process whereby arbitrary information is encoded into an image in such a way that the additional payload is imperceptible to the image observer[29].

Digital watermarking is a form of data hiding or steganography. Motivated by growing concern about the protection of intellectual property on the Internet and by the treat of a ban for encryption technology, the interest of watermarking techniques has been increasing over the recent years [23]. In a digital image watermarking system, information carrying watermark is embedded in an original image. The watermarked image is then transmitted or stored. The received watermarked image is then decoded to resolve the watermark. The general watermarking system flowchart is sketched in Fig 1.2.

Watermarking and cryptography encryption are closed related in the spy craft family. Cryptography scrambles a message so it cannot be understood. A watermarking method hides the message so it cannot be seen, a message in ciphertext might cause suspicion on the recipient while an invisible message created with steganographic methods will not. Note that watermarking is distinct from encryption. Its goal is not to restrict or regulate access to the host signal, but to ensure that embedded data remain inviolate and recoverable [23]. There is little protection for decrypted or descrambled content, which can be redistributed or misappropriated. Digital watermarking is intended by its developers as the solution to the need to provide value added protection on top of data encryption and scrambling for content protection.

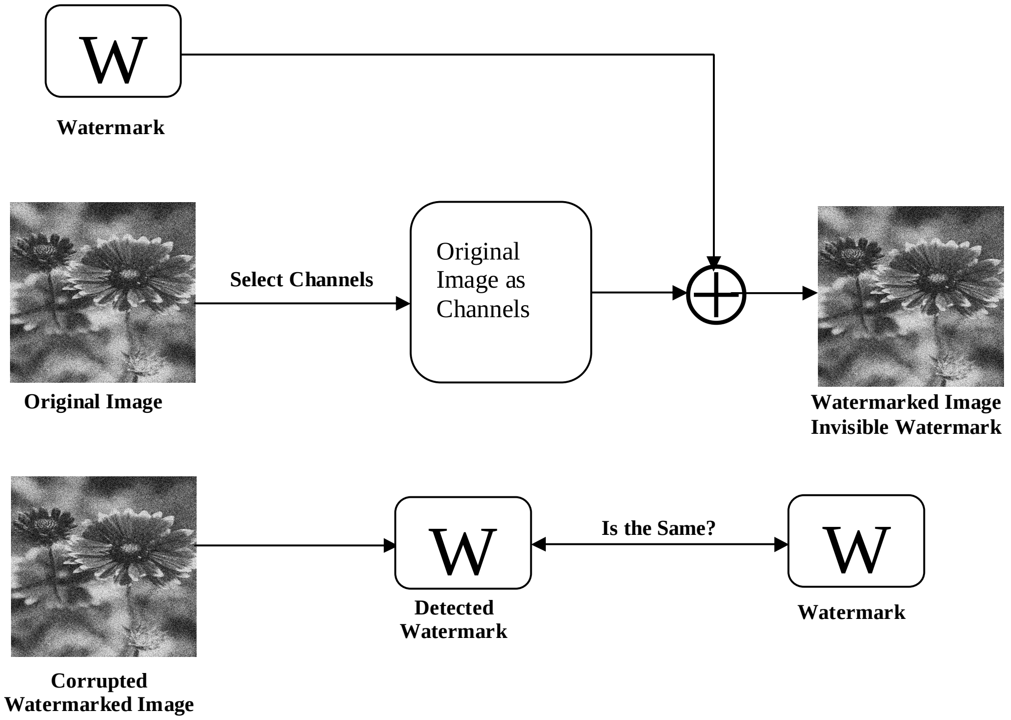


Figure 1.2. A General Watermarking System

Today, crypto graphical techniques have reached a level of sophistication such that properly encrypted communications can be assumed secure well beyond the useful life of the information transmitted. In fact, it’s projected that the most powerful algorithms using multi kilobit key lengths could not be comprised through brute force, even if all the computing power worldwide for the next twenty years was focused on the attack. Of course the possibility exists that vulnerabilities could be found, or computing power breakthroughs could occur, but for most users in most applications, current cryptographic techniques are generally sufficient.

Why then pursue the field of information hiding? Several good reasons exist, the first being that “security through obscurity” isn’t necessarily a bad thing, provided that it isn’t the only security mechanism employed. Steganography for instance allows us to hide encrypted messages in mediums less likely to attract attention. A garble of random characters being transmitted between two users may tip off a watchful third party that sensitive information is being transmitted; whereas baby pictures with some additional noise present may not. The underlying information in the pictures is still encrypted, but attracts far less attention being distributed in the picture than it would otherwise. This becomes particularly important as the technological disparity between individuals and organizations grows. Governments and businesses typically have access to more powerful systems and better encryption algorithms then individuals. Hence, the chance of individual’s messages being broken increases which each passing year. Reducing the number of messages intercepted by the organizations as suspect will certainly help to improve privacy.

C. Basic Principles of Watermarking

All watermarking methods share the same generic building blocks, a watermark embedding system and a watermark recovery. Fig 1.3 shows the generic watermark embedding process. The input to the scheme is the watermark, the cover-data and an optional public or secret key. The watermark can be of any nature such as a number, text, or an image. The key may be used to enforce security that is the prevention of unauthorized parties from recovering and manipulating the watermark. All practical systems employ at least one key, or even a combination of several keys[10,6].

Imperceptibility The modifications caused by watermark embedding should be below the perceptible threshold, which means that some sort of perceptibility criterion should be used not only to design the watermark, but also quantify the distortion. As a consequence of the required imperceptibility, the individual samples (or pixels, features, etc.) that are used for watermark embedding are only modified by a small amount.

Redundancy To ensure robustness despite the small allowed changes, the watermark information is usually redundantly distributed over many samples (or pixels, features, etc.) of the cover-data, thus providing a global robustness which means that the watermark can usually be recovered from a small fraction of the watermarked data. Obviously watermark recovery is more robust if more of the watermarked data is available in the recovery process.

Keys In general, watermarking systems use one or more cryptographically secure keys to ensure security against manipulation and erasure of the watermark. As soon as a watermark can be read by someone, the same person may easily destroy it because not only the embedding strategy, but also the locations of the watermark are known in this case. These principles apply to watermarking schemes for all kinds of data that can be watermarked, like audio, images, video, formatted text, 3D models, model animation parameters, and others. The generic watermark recovery process is depicted in Fig 1.4. Inputs to the scheme are the watermarked data, the secret or public key and, depending on the method, the original data and/or the original watermark. The output is either the recovered watermark W or some kind of confidence measure.

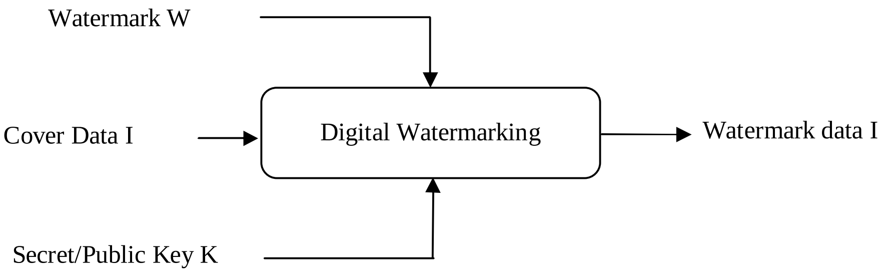


Figure 1.3 Generic Watermarking Schemes

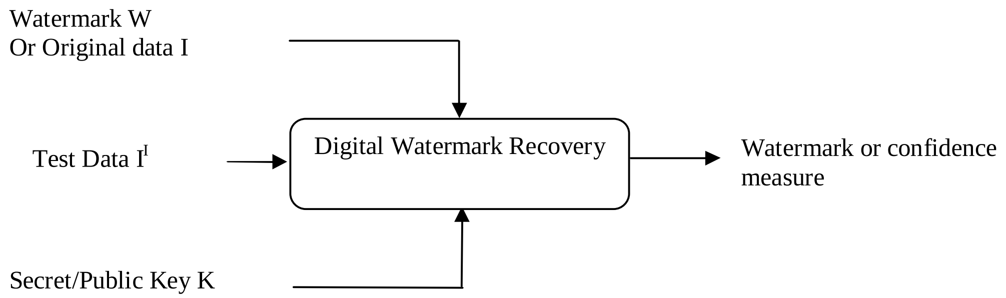


Figure 1.4 Generic Watermark Recovery Scheme

II. BACKGROUND INFORMATION

Digital watermarking, which is hiding useful information pertaining to the owner or the content creator, was initially used in paper and money as measure of genuineness. Although as a means of authentication of digital content may not prevent unauthorized use, it certainly is a mechanism to track the owner of the digital content. Digital Rights Management techniques are being researched to establish more secure protocol to safeguard the information as well as control their distribution [7]

It is apparent that copying will always takes place therefore a method of identifying the route of copied media could be appealing. It is mainly desirable to detect whether a file is the original and also to whom the original belongs. Publishers are reluctant to distribute material electronically, so they would like a method of applying a digital watermarking to their productions for copyright reasons [11].

Consider a company producing media for sale, for example 3D models; a customer wishes to identify that the model they have purchased is the original unmodified object from the company. If the model has been modified it may be maliciously to ensure the model does not adhere to the requirements specification therefore meaning another model to be sought from a competitor. Perhaps an author produces forms of media and wishes them to be copyrighted against unauthorized use or distribution. There must be a method for determining the original author of a file for copyright laws to be enforced in the court of law. With these requirements, a relatively old technique known as watermarking has been adapted for use in the modern age[21].

Unlike printed watermarks, digital watermarking is a technique where bits of information are embedded in such a way that they are completely invisible. The problem with the traditional way of printing logos or names is that they may be easily tampered or duplicated. In digital watermarking, the actual bits are scattered in the image in such a way that they cannot be identified and show resilience against attempts to remove the hidden data. Traditional watermarking involved small visible marks in paper to ensure their originality or that they are official. Examples of this can be found in government cheques, official documents and paper money. This method has been modified and updated for digital images and similar techniques are also used for digital video, audio and text[19].

Digital watermarks may be perceptible or imperceptible. Imperceptible watermarks cannot be detected by the human senses, but can be read by a computer. Many authors feel that image based digital watermarks should be invisible to the human eye. If the watermark is supposed to be imperceptible, there is a debate as to whether the existence of the watermark should be advertised. Advertising the presence of watermarks invites hackers to attempt to alter or disable them. If media can be manipulated by legitimate means to embed a watermark, illicit information can also be placed in the same imperceptible space. Other authors prefer visible watermarks, and clearly advertise the existence of watermarks, to deter illicit handling or theft of the images. Both viewpoints have merit, but the determination must be made by the owner of the images and depends on the intended use of the watermarked work. Some watermarking techniques can be used to determine if there has been any tampering with the work; other watermarking methods may be used to track works to and from licensed users.

Another classification depends on whether the watermark is applied in the space domain or in a transform domain. Tools used in the space domain include bit-wise techniques such as least significant bit or noise insertion and manipulation. Patterns placed in the image and spatial relationships between image components are other additive forms of watermarking. Techniques that provide additive information such as masking techniques without applying a function of the image to determine the watermark location are also categorized as being in the space domain, though they share the survivability properties of transform domain techniques. The transform domain class of watermarks includes those that manipulate image transforms.

Many variations on this transforms domain approaches exist, ranging from applying the transform to the entire image to applying it to blocks of the image. These methods hide messages in relatively significant areas of the cover and may manipulate image properties such as luminance. Transform domain watermarking and masking techniques are more robust to attacks such as compression, cropping, and image processing techniques in which significant bits are changed. Both spatial domain and transform domain methods may employ patchwork, pattern block encoding, or spread spectrum concepts which may add redundancy to the hidden information. These approaches help protect against some types of image processing such as cropping and rotating.

A. Steganography

Steganography is the study of techniques for hiding the existence of a secondary message in the presence of a primary message. The primary message is referred to as the carrier signal or carrier message; the secondary message is referred to as the payload signal or payload message. Classical Steganography can be divided into two areas, technical steganography and linguistic steganography. The classification of the various steganographic techniques is shown in Fig 2.2 and described briefly in the following section.

Technical steganography involves the use of technical means to conceal the existence of a message using physical or chemical means. Examples of this type of steganography include invisible inks, which have been known since antiquity or more recently, photomechanical reduction resulting in so-called microdots that permit the reduction of a letter-sized page onto an area of photographic film no larger than the dot at the end of this sentence.

Linguistic steganography itself can be grouped into two categories, open codes and semagrams. The latter category also encompasses visual semagrams. These are physical objects, depictions of objects or other diagrams with an ostensibly innocuous purpose in which a message is encoded. Examples of semagrams include the positioning of figures on a chessboard. Text semagrams are created by modifying the appearance of a text in such a way that the payload message is encoded.

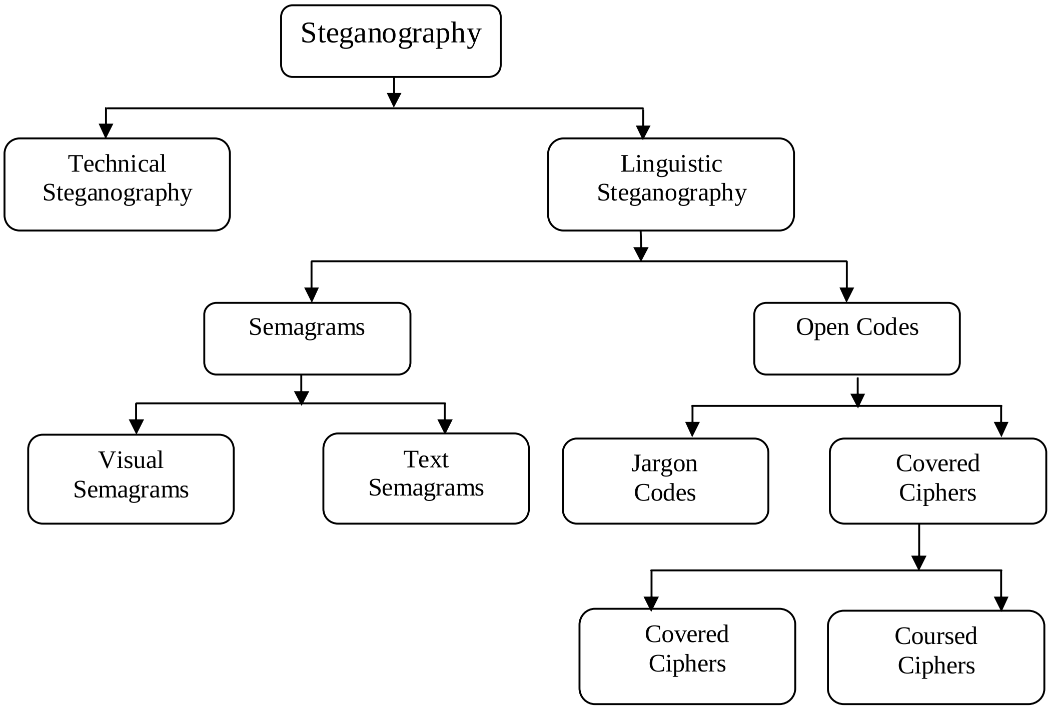


Figure 2.2 Classifications of Steganographic Techniques

The category of open codes is characterized by embedding the payload signal in such a way in the carrier signal that the carrier signal itself can be seen as a legitimate message from which an observer may not immediately deduce the existence of the payload signal.

One of the most frequently cited examples is the cue code with which World War II Japanese diplomats were to be notified of impending conflict. In this code, “HIGASHI NO KAZE AME” (“east wind, rain”) signified pending conflict with the United States, while “KITANO KAZE JUMORI” (“north wind, cloudy”) indicated no conflict with the U.S.S.R. and “NISHI NO KAZE HARE” (“west wind, clear”) with the British Empire1. Unlike jargon codes, which lead to atypical language that can be detected by an observer, cue codes are harder to detect provided that their establishment has not been compromised.

B. Watermarking

Although cryptography and watermarking both describe techniques used for covert communication, cryptography typically relates only to covert point to point communication between two parties. Cryptography methods are not robust against attacks or modification of data that might occur during transmission, storage or format conversion. Watermarking, as opposed to cryptography, has an additional requirement of robustness against possible attacks. An ideal cryptographic system would embed a large amount of information securely, with no visible degradation to the cover object. An ideal watermarking system, however, would embed an amount of information that could not be removed or altered without making the cover object entirely unusable. As a side effect of these different requirements, a watermarking system will often trade capacity and perhaps even some security for additional robustness.

The working principle of the watermarking techniques is similar to the cryptography methods. A watermarking system is made up of a watermark embedding system and a watermark recovery system. The system also has a key which could be either a public or a secret key. The key is used to enforce security, which is prevention of unauthorized parties from manipulating or recovering the watermark.

III. FHT ORIENTED DIGITAL IMAGE WATERMARKING

Digital media offers several advantages over analog media, such as high quality, easy editing, high fidelity copying. The ease by which digital information can be duplicated and distributed has led to the need for effective copyright protection tools. Various techniques have been recently introduced in attempt to address these growing concerns. These techniques hiding data within digital images, audio and video files. One way such data hiding is digital watermark that completely characterizes the person who applies it and, therefore, marks it as being his intellectual property. A great deal of research efforts has been focused on Digital image watermarking in the recent years. Fast Hadamard Transform is one of the up growing frequency domain digital watermarking technique.

A. Fast Hadamard Transform

In the past decade fast orthogonal transforms have been widely used in many areas, such as data compression, pattern recognition and image reconstruction, interpolation, linear filtering, spectral analysis, cryptography, watermarking and communication systems. The computation of unitary transforms is a complicated and time consuming task. However, it would not be possible to use the orthogonal transforms in signal and image processing application without effective algorithms calculating them. An important question in many applications is how to achieve the highest computation efficiency of the discrete orthogonal transforms.

Among discrete orthogonal transforms a special role plays a class of Hadamard transforms based on the Hadamard matrices ordered by Hadamard, Walsh and Paley. These matrices are known as non-sinusoidal orthogonal transform matrices and have found applications in digital signal processing and communication systems as they do not require any multiplication operation in their computation. It performs an orthogonal, symmetric, involuntary, linear operation on 2^m real numbers. Recently, Hadamard transforms and their variations have found a widely usage in watermarking[7].

Fast Transforms: The problem of computing a transform has been extensively studied. Methods to perform a discrete orthogonal transform with an essentially smaller number of operations than direct matrix multiplication, i.e. so-called fast transforms.

In general, a fast transform $T_N f$ may be achieved by factoring the transform matrix T_N by the multiplication of k sparse matrices. Typically, $N=2^n$, $k= log_2N=n$, and $T_{2n}=F_n$, F_{n-1}, $…F_1$, Where F_i are very sparse matrices so that the complexity of multiplying by F_i is $O(N)$, $i=1,2,..n$. $N=2^n$-point inverse transform matrix $T^{-1}{}_N$ can be represented as: $T_{2^n}^{-1} = T_{2^n}^T = (F_n F_{n-1} ... F_1)^T = F_1^T F_2^T ... F_n^T$. Thus, one can implement the transform T_Nf via the following consecutive computations $f \rightarrow F_1f \rightarrow F_2(F_1f) \rightarrow … \rightarrow F_n(…F_2(F_1f)…))$.

Based on this factorization the computational complexity is reduces from $O(N)$ to $O(NlogN)$. Since F_i contains only few nonzero terms per row, the transformation T_Nf can be efficiently accomplished be operation on fn times. For Hadamard F_i contains only two nonzero terms in each row. So an N-point one dimensional transform with above given decomposition can be implemented in $O(NlogN)$ operations, which is far fewer than N^2 operations. Since the Walsh-Hadamard transform functions assume only the value -1 and +1, their computation requires only additions and subtractions.

Definition**:** The Hadamard transform H_m is a $2^m \times 2^m$ matrix, the Hadamard Matrix that transforms 2^m real numbers X_n into 2^m real numbers X_k. We can define the Hadamard transform in two ways: recursively or by using the binary representation of the indices n and $k[2]$.

An *n x n* matrix $H= h_{ij}$ is a Hadamard matrix of order *n* if the entries of *H* are either +1 or -1 and such that $HH^T= I$ where H^T is the transpose of *H* and *I* is the order *n* identity matrix. In other words, an *n x n* matrix with only +1 and -1 elements.

Recursively, we define the 1x1 Hadamard transform H_0 by the identity $H_0 = 1$, and then define H_m for $m > 0$ by:

$$H_m = \frac{1}{\sqrt{2}} \begin{bmatrix} H_{m-1} & H_{m-1} \\ H_{m-1} & -H_{m-1} \end{bmatrix}$$

Where the $\frac{1}{\sqrt{2}}$ is a normalization that is sometimes omitted. Thus, other than this normalization factor, the Hadamard matrices are made up entirely of +1 and −1. Equivalently, we can define the Hadamard matrix by its *(k, n)*- th entry by writing $k=k_{m-1}2^{m-1} + k_{m-2}2^{m-2}+....+k_1 2+k_0$ and $n=n_{m-1}2^{m-1}+n_{m-2}2^{m-2}+...+n_1 2+n_0$, where the k_j and n_j are the binary digits (0 or 1) of *n* and *k*, respectively. In this case, we have: $(H_m)_{k,n} = \frac{1}{2^{m/2}}(-1)\sum_j k_j n_j$

This is exactly the multi-dimensional $2\times 2\times 2 ......\times 2$ DFT, normalized to be unitary, if we regard the inputs and outputs as multidimensional arrays indexed by the n_j and k_j, respectively.

Let *H* be a Hadamard matrix of order n. Then the partitioned matrix

$$\begin{bmatrix} H & H \\ H & -H \end{bmatrix}$$

is a Hadamard matrix of order *2n*. This observation can be applied repeatedly and leads to the following sequence of matrices, also called Walsh matrices

$$H_1 = [1]$$

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

and

$$H_{2^k} = \begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix} = H_2 \otimes H_{2^{k-1}}$$

for, $2 \le k \in N$ where ⊗ denotes the Kronecker product, A few examples of Hadamard matrices are

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

These matrices were first considered as Hadamard determinants because the determinant of a Hadamard matrix satisfies equality in Hadamard's determinant theorem, which states that if $X=x_{ij}$ is a matrix of order n *where* $|x_{ij}| \le 1 \ \forall\, i$ and *j* then $det(X) \le n^{n/2}$

Kronecker product: For any two arbitrary matrices A and B, we have the direct product or Kronecker product A ⊗ B defined as

$$\begin{bmatrix} a_{11}B & a_{12}B & . & . & a_{1n}B \\ . & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & . \\ a_{m1}B & a_{m2}B & . & . & a_{mn}B \end{bmatrix}$$

Note that if A is m-by-n and B is p-by-r then A ⊗ B is an mp-by-nr matrix. Again this multiplication is not commutative. For example

$$\begin{bmatrix}1 & 2\\3 & 1\end{bmatrix}\otimes\begin{bmatrix}0 & 3\\2 & 1\end{bmatrix}=\begin{bmatrix}1.0 & 1.3 & 2.0 & 2.3\\1.2 & 1.1 & 2.2 & 2.1\\3.0 & 3.3 & 1.0 & 1.3\\3.2 & 3.1 & 1.2 & 1.1\end{bmatrix}=\begin{bmatrix}0 & 3 & 0 & 6\\2 & 1 & 4 & 2\\0 & 9 & 0 & 3\\6 & 3 & 2 & 1\end{bmatrix}$$

If A and B represent linear transformations $V_1 \rightarrow W_1$ and $V_2 \rightarrow W_2$, respectively, then A ⊗ B represents the tensor product of the two maps, $V_1 \otimes V_2 \rightarrow W_1 \otimes W_2$

Properties of the Hadamard Transform matrices.

1. The Hadamard transform H is real, symmetric, and orthogonal, that is $H=H^*=H^T=H^{-1}$
2. The Hadamard transform is a fast transform.
3. The natural order of the Hadamard transform coefficients turns out to be equal to the bit reversed gray code representation of its sequences.
4. Hadamard transform has well to very good energy compaction for highly correlated images.

IV. FHT DIGITAL WATERMARKING

In this Watermarking system design, the first step to be considered is the embedding of the watermark. Traditionally the watermark should not be placed in perceptually insignificant regions of the image (spatial) or its frequency spectra. The reason is that many signal and geometrical processes affect these components.

A watermark placed in the high frequency spectrum of an image can be easily destroyed with little degradation by direct or indirect low-pass filtering. On the other hand the low-pass components of an image should not be altered for two reasons. First as most of the image energy is concentrated in the low frequency components, any appreciable change may cause fidelity loss. Secondly, the energy of these low frequency components could be considered as noise and thus subtracted, in the case that the original image is available. But in the absence of the original image, the image noise creates great concern during the detection phase. One of the solutions to this problem is to apply matched filtering before correlation. This decreases the contribution of the original to the correlation, or to select low to middle level of coefficients.

In this scheme each component of color space is considered as an independent communication channel and the Watermark as a narrow band signal, communicated over larger bandwidth signals. Here, the watermark sequence consists of real numbers generated by a random number generator. Random generator makes the watermark difficult for an attacker to estimate it from marked media and even if the attacker can estimate some segments of the watermark, it is not possible to determine the rest of the watermark[15,16,7]. The FHT embedding algorithm provides a robust and efficient approach to perform digital watermarking of digital image data for copyright protection and proof of rightful ownership.

2D-Hadamard transform of signal The 2D-Hadamard transform has been used extensively in image processing. Let *[U]* represents the original image and *[V]* the transformed image, the 2D-Hadamard transform is given by $[V]=\frac{Hn[U]Hn}{N}$

Where H_n represents and N x N Hadamard matrix, $N=2n$, $n=1, 2, 3$….with element values either +1 or -1. The advantages of Hadamard transform are that the elements of the transform matrix H_n are simple. They are binary, real numbers and the rows or columns of H_n are orthogonal. Hence the Hadamard transform matrix has the following property: $H_n=H_n^*=H^T=H^{-1}$

Since H_n has N orthogonal rows $H_nH_n=NI$ (I is identity matrix) and $H_nH_n=NH_nH_n^{-1}$, thus $H^{-1}=\frac{H_n}{N}$ The inverse 2D-fast Hadamard transform (IFHT) is given as

$$[U]=H_n^{-1}[V]H_n^*$$
$$=\frac{\mathrm{H}_\mathrm{n}[V]H_n}{N}$$

The Hadamard matrix of the order n is generated in terms of Hadamard matrix of order n-1 using Kronecker product ⊗, as $\mathrm{H}_\mathrm{n} = \mathrm{H}_{\mathrm{n}-1} \otimes \mathrm{H}_1$ or $H_n=\begin{bmatrix}H_{n-1} & H_{n-1}\\H_{n-1} & -H_{n-1}\end{bmatrix}$

In this algorithm, the processing is performed based on 8x8 sub-blocks of the whole image, the third order Hadamard transform matrix H_3 is used.

$$H_3 \quad = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix}$$

For a H_3 matrix, the no of transitions for row1 to row 8 is 0,7,3,4,1,6,2 and 5.The number of sign changes is referred to as sequency .The concept of sequency is analogous to frequency for the Fourier Transform. Zero sign transitions correspond to a DC component. While a large number of sign transitions correspond to high frequency components. For a Hadamard matrix H_3, the elements are not arranged in an increasing sequency, such that the transitions are 0,1,2,3,4,5,6 and 7[15,16,7]

A. Fht Oriented Watermarking Algorithms

The 2D Hadamard transform has been used with a great success in image watermarking and image compression. Hadamard transform take only the binary values +1 and -1. Hence, the FHT is well suited for digital image processing applications where computational simplicity is required. Let V be the original image of size N × N. The 2D Hadamard transform of *V* is given by $U = \frac{(HVH)}{N}$, where H is a Hadamard matrix of order N = 2n (n is an integer), and with entries {−1, +1}. The Hadamard matrix H has mutually orthogonal rows or columns, and satisfies $HH^T = NIN$, where *IN* is the identity matrix. Hence, the original image may be recovered using $V = \frac{(HUH)}{N}$. Furthermore, the Hadamard matrix of order N may be generated from the Hadamard matrix of order $\frac{N}{2}$ using the Kronecker product property $HN = H_2 \otimes \frac{HN}{2}$, where H_2 is the Hadamard matrix of order $N = 2$.

Here provide the main steps of the watermark embedding and extraction algorithms which are also illustrated in the block diagrams shown in Fig 5.1 and 5.2.

1) Watermark Embedding Algorithm

FHT Embedding Algorithm

Input : Original Image (is denoted by *f(x,y))* ,watermark Image (is denoted by *w(x,y))*

Output : Watermarked Image

Step 1: Watermark image(watermark) $w(x, y)$ is transformed into FHT coefficients. After transformation, *16×16* watermark, Hadamard transform coefficients are obtained. In this algorithm use image of size *16×16* as a watermark and image of size *256×256* as a original image for testing. Here the DC component is stored in a key file and the AC components are then selected for embedding.

Step 2: The original image $f(x, y)$, is also decomposed into a set of non-overlapped blocks of $h\times h$, denoted by $f_k(x^1, y^1)$, $k=0, 1, \ldots,$ $\boldsymbol{K}$*-1*, Where the subscript k denotes the index of blocks and $\boldsymbol{K}$ denotes the total number of blocks. In this experiment, a test image of size 256×256 and sub-block size of 8×8 is used.

Step 3: This Fast Hadamard Transforms algorithm, pseudo randomly selects the sub-blocks from the original image by using java-sequence random number for watermark insertion

Step 4: The seed of this java-sequence and initial state are also stored in the key file. After that, a FHT is performed on each selected sub-blocks of the original image. Since the sub-block size is 8×8, a Hadamard transform of matrix size H_3 is used. For each 8×8 sub-block, 16 Hadamard transform coefficients are obtained.

Step 5: Let the watermark FHT coefficients denote by m_i. The AC components of FHT coefficients of the original image sub-blocks, before and after inserting watermark are denoted by x_i, and x_i* respectively. Where $i \in (0,n)$, with n the number of the watermarked coefficients which is 16 in this experiment. The watermark strength factor is denoted by α.. The embedding formula is $\boldsymbol{X_i{*}=\alpha m_i}$ The original coefficient X_i is replaced by X_i*.

Here α. is strength factor and its formula is $\alpha=\beta{*}mask\ _1(j, k)\ {*}\ mask\ _2(j, k)$ Where β is the scaling factor, j and k indicate the positions of the sub-blocks. The watermark strength factor α can be adaptively controlled according to the texture areas. High textured areas are watermarked with higher strength. Outstanding edge areas and smooth areas are watermarked with less strength. In this way, the invisibility of the watermarked image can be improved.

Step 6: After the watermark insertion, a new 8×8 matrix of FHT coefficients is obtained. The InverseFHT is then applied to the 8×8 matrix using equation $[V]=\dfrac{(H_n[U]H_n)}{N}$ to obtain the luminance value matrix of the watermarked image sub-block $f_k^1(x^1,y^1)$.

Step 7: After performing the watermark insertion for all the relevant sub-blocks of the original image, the watermarked image $f^1(x, y)$ is obtained. At the same time, a key file is also generated, which is needed for the decoding process.

2) *Watermark Extraction Algorithm*

FHT Extraction Algorithm

Input : Watermarked Image (is denoted by $f^{11}(x, y)$)

Output : Extracted Watermark

Step 1: Transforming all the relevant sub-blocks, $f_k^{11}(x^1, y^1)$, into the FHT domain, Here obtain all the Hadamard transform coefficients embedded with the watermark.

Step 2: In each of the sub- block FHT coefficients, the watermark bits are inserted into the bottom right sixteen middle and high frequency components. Let these components denote by $X_i{*}^1$, the retrieved watermark FHT coefficients denote by m_i^1, where $i \in (0,n)$, and the number of the watermarked coefficients n = 16.

Step 3: The watermark extraction formula is given as: $m_i^1 = \dfrac{X_i^{*1}}{\alpha}$ Where α is strength factor and its formula is $\boldsymbol{\alpha=\beta\ {*}\ mask\ _1(j, k)\ {*}\ mask\ _2(j, k)}$, Where β is the scaling factor, j and k indicate the positions of the sub-blocks.

Step 4: The watermark FHT coefficients are extracted from all the sub-blocks of the original image. Along with the DC component stored in the key file, the AC coefficients are rearranged into a 16×16 FHT coefficients matrix.

Step 6: The extracted watermark image, $w(x,y)$, is obtained by Inverse FHT of the 16×16 Hadamard coefficients matrix using equation $[V]=\dfrac{(H_n[U]H_n)}{N}$.

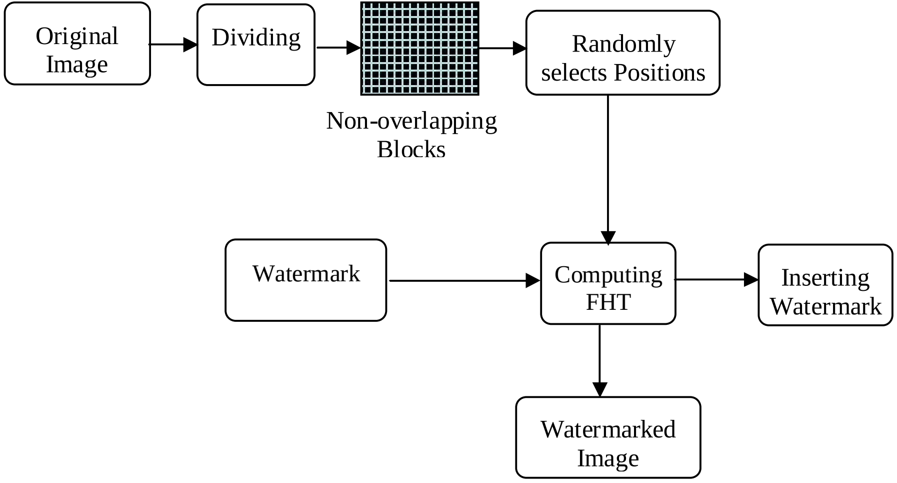


Figure 3.1 Image-In-Image Watermark embedding Process

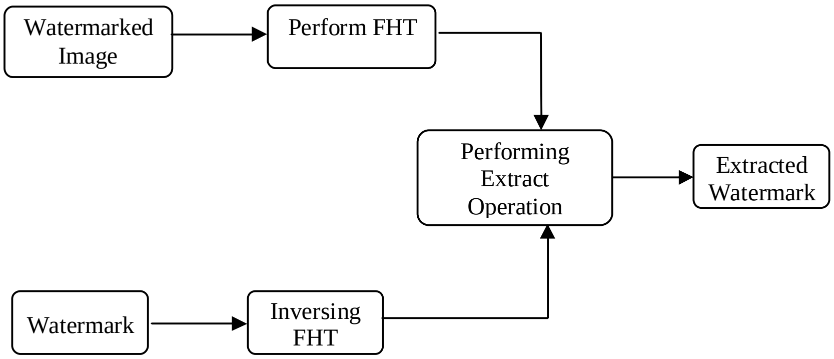


Figure3.2 Image-In-Image Watermark Extraction Process

V. WATERMARK STRENGTH FACTOR

The determination of the watermark strength factor is based on the original image textures and edges characteristic. The classification of different areas is based on the Hadamard transformed space energy analysis and canny edge detection algorithm. The first visual mask model is determined by the Hadamard transformed space image energy distribution. The analysis is performed on the FHT coefficients of sub-blocks for watermarking. For coarse texture and outstanding edge areas, most of the signal energy is concentrated in the AC components of the Hadamard transform for smooth areas, the energy is mainly concentrated in the low AC and DC components. Here use a squared sum of AC components to generate this visual mask, $mask_1(j, k)$ to distinguish the smooth and coarse texture areas. Counting the number of edge points in each sub-block, here obtain another visual mask, $mask_2(j,k)$.This mask is used to determine the coarse texture or outstanding edge in the image block. Large values in this mask indicate that the corresponding block is highly textured. Smaller values indicate that the block contains outstanding edges .The two mask values are multiplied and scaled to a specific range. The water mark strength factor α is obtained as follows: $\alpha=\beta * mask_1(j, k) *mask_2(j, k)$, Where β is scaling factor, j and k indicate the positions of the sub-blocks. The watermark strength factor α can be adaptively controlled according to the texture areas. High textured areas are watermarked with higher strength. Outstanding edge areas and smooth areas are watermarked with less strength. In this way, the invisibility of the watermarked image can be improved.

A. Analysis Of Results

The experiment for the watermarking insertion system is performed using the Java 1.5. Two container test images consist of orginal.jpg and logo.jpg are used. These images are of sizes of 256×256×8bit. For this algorithm, a maximum image size of 16×16 bit can be hidden into the container image of size 256x256x8bit. The original and watermarked image examples are shown in below figure.

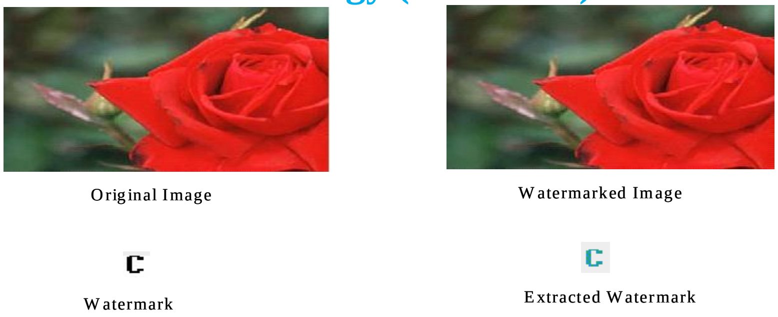
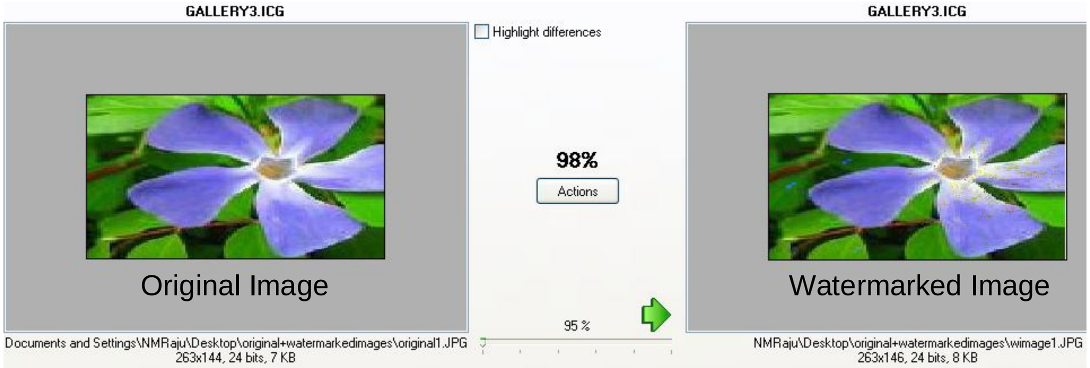


Figure 3.3 Image-In-Image Watermarking Insertion & Extraction

Comparison of Original image with watermarked images (Tested Images are shown in following Figures). The comparison is using Image comparer 3.5 version. It compares original image and watermarked image and display the equality percentage. It can also display distortion areas between original image and watermarked image. The Results are shown in the following table.

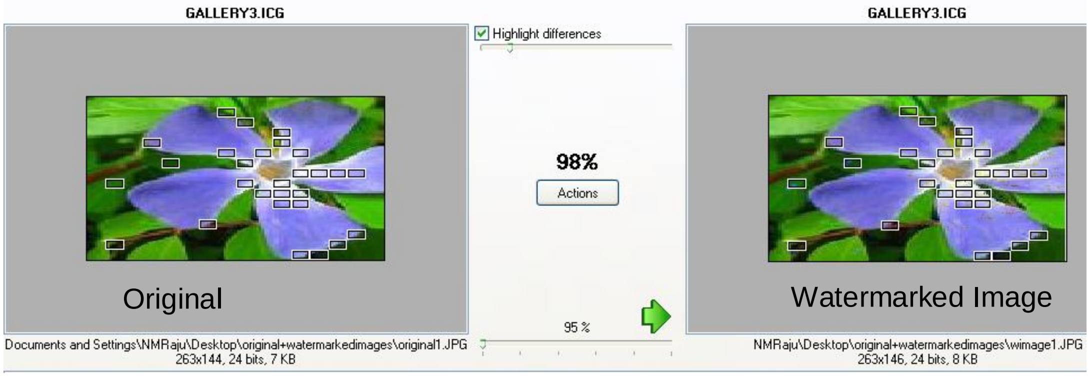
Name	Equality Percentage (Out of 100 %)	Difference Percentage
Original1.jpg, Watermark1.jpg	98%	2%
Original2.jpg, Watermark3.jpg	99%	1%
Original3.jpg, Watermark3.jpg	99%	1%
Original4.jpg, Watermark4.jpg	99%	1%

5.1. Analysis of Results



Documents and Settings\NMRaju\Desktop\original+watermarkedimages\original1.JPG
263x144, 24 bits, 7 KB

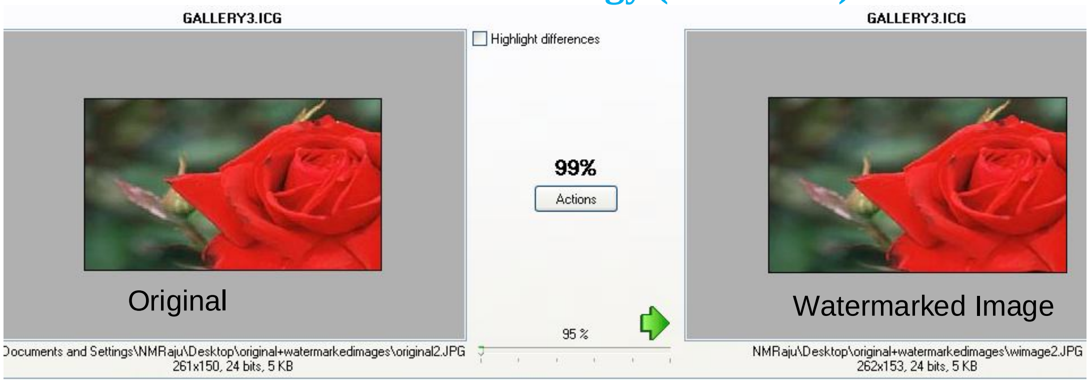
NMRaju\Desktop\original+watermarkedimages\wimage1.JPG
263x146, 24 bits, 8 KB



Documents and Settings\NMRaju\Desktop\original+watermarkedimages\original1.JPG
263x144, 24 bits, 7 KB

NMRaju\Desktop\original+watermarkedimages\wimage1.JPG
263x146, 24 bits, 8 KB

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

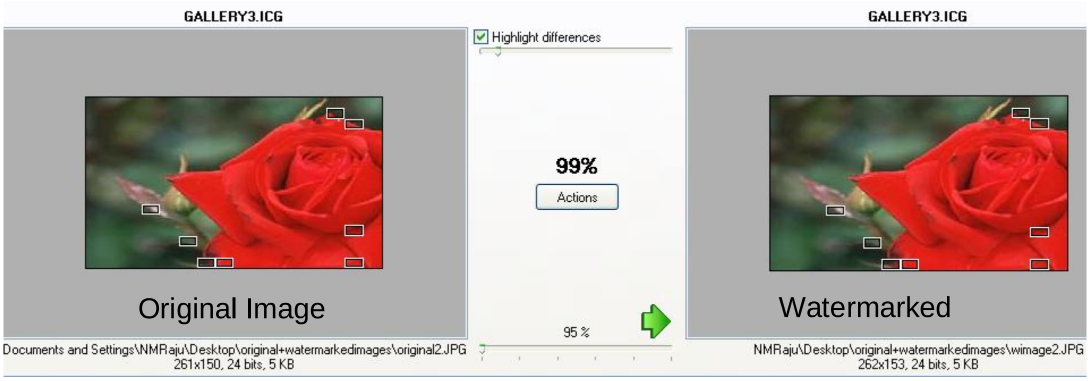


Original

Watermarked Image

Documents and Settings\NMRaju\Desktop\original+watermarkedimages\original2.JPG
261x150, 24 bits, 5 KB

NMRaju\Desktop\original+watermarkedimages\wimage2.JPG
262x153, 24 bits, 5 KB

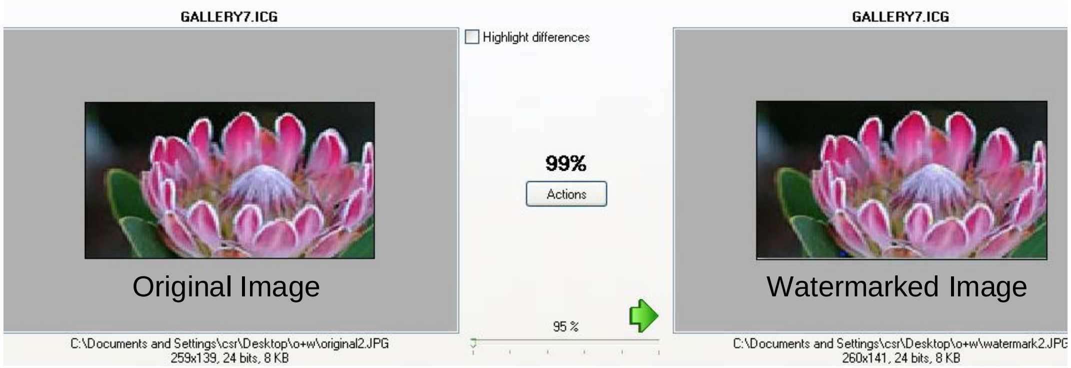


Original Image

Watermarked

Documents and Settings\NMRaju\Desktop\original+watermarkedimages\original2.JPG
261x150, 24 bits, 5 KB

NMRaju\Desktop\original+watermarkedimages\wimage2.JPG
262x153, 24 bits, 5 KB

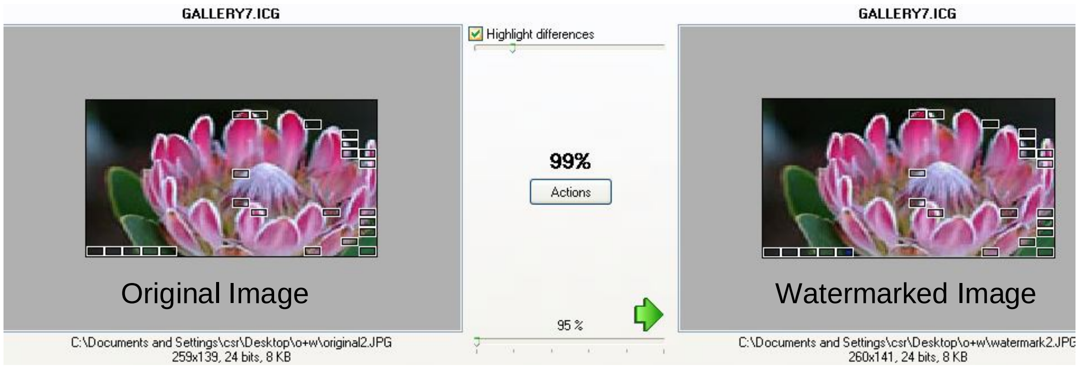


Original Image

Watermarked Image

C:\Documents and Settings\csr\Desktop\o+w\original2.JPG
259x139, 24 bits, 8 KB

C:\Documents and Settings\csr\Desktop\o+w\watermark2.JPG
260x141, 24 bits, 8 KB

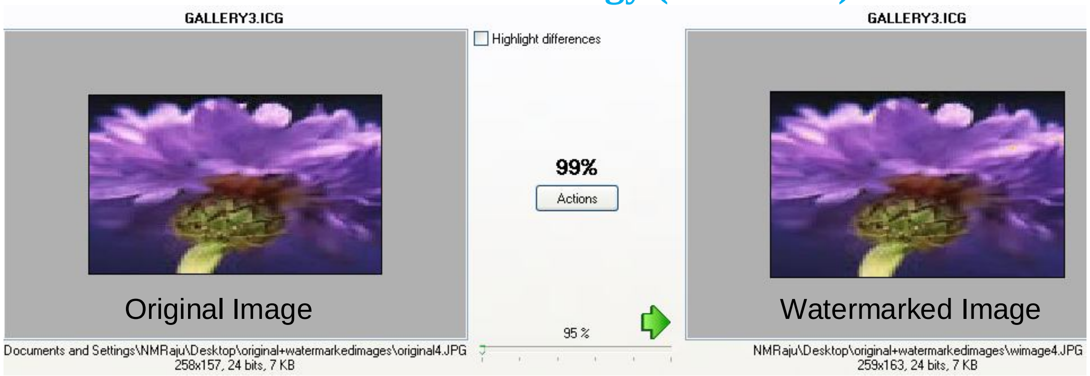


Original Image

Watermarked Image

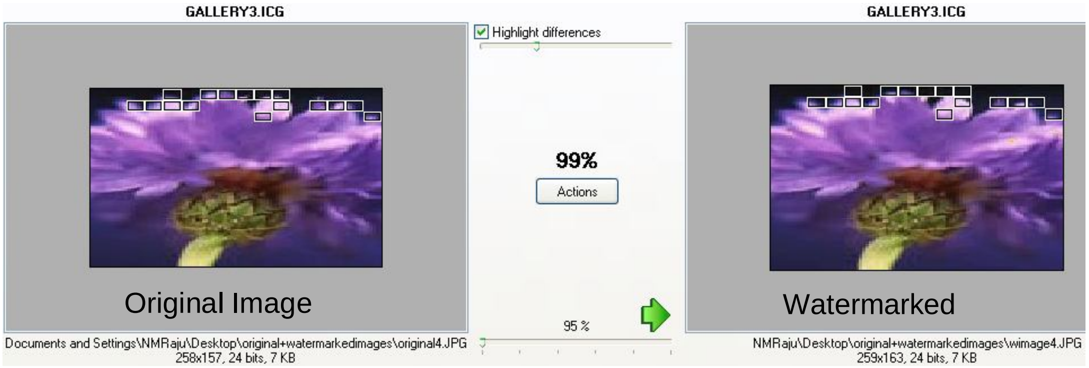
C:\Documents and Settings\csr\Desktop\o+w\original2.JPG
259x139, 24 bits, 8 KB

C:\Documents and Settings\csr\Desktop\o+w\watermark2.JPG
260x141, 24 bits, 8 KB



Documents and Settings\NMRaju\Desktop\original+watermarkedimages\original4.JPG
258x157, 24 bits, 7 KB

NMRaju\Desktop\original+watermarkedimages\wimage4.JPG
259x163, 24 bits, 7 KB



Documents and Settings\NMRaju\Desktop\original+watermarkedimages\original4.JPG
258x157, 24 bits, 7 KB

NMRaju\Desktop\original+watermarkedimages\wimage4.JPG
259x163, 24 bits, 7 KB

VI. CONCLUSIONS AND FUTURE WORK

In this paper, we introduce an Efficient Fast Hadamard Transforms oriented Digital Image-In-Image Watermarking, which offers better solution to copyright protection and provide more security from various attacks. The Hadamard transform has more useful middle and high frequency bands than several high gain transforms, such as Discrete Cosine Transforms, Discrete Wavelet Transforms. FHT also offers significant advantage in terms of shorter processing time and the ease of hardware implementation than many common transform techniques. In future to develop a truly robust, transparent and secure watermarking technique for different digital media including images, video and audio.

REFERENCES

[1] Adrian G. Bors and Ioannis Pitas , “Image watermarking using block site selection and DCT domain constraints”, Department of Informatics, University of Thessaloniki, Thessaloniki54006,Greece.

[2] Bogdan J F, Susanto R., "Complex Hadamard Transforms: Properties, Relations and Architechture", Proceedings of IEICE Transactions on Fundamentals, Volume- 87-A, Issue.8, August 2004.

[3] Ching-Yung Lin, Shih-Fu Chang;” SARI: Self-Authentication-and-Recovery Image Watermarking System”, ACM Multimedia 2001, Ottawa, Canada, Sep. 30 - Oct 5, 2001.

[4] Chiou-Ting Hsu and Ja-Ling Wu., “Hidden Digital Watermarks in Images”, IEEE Transactions on Image Processing, Volume. 8, Issue. 1, January 1999.

[5] Christian R, Jean Luc D., “A Survey of Watermarking Algorithms for Image Authentication”, EURASIP Journal on Applied Signal Processing, pp.613–621, 2002.

[6] Christine I P and Edward J D, "Digital Watermarking Algorithms and Applications", IEEE Signal Processing Magazine, July 2001.

[7] Emad E. Abdallah, Hamza Ben A, Bhattacharya P., “A Robust Block-based Image Watermarking scheme using Fast Hadamard Transform and Singular Value Decomposition”, Proceedings of The 18th International Conference on Pattern Recognition, Volume 3,pp.673-676,2006.

[8] Eugene T. Lin and Edward J. Delp., “A Review of Data Hiding in Digital Images”, Video and Image Processing Laboratory, School of Electrical and Computer Engineering, Purdue University, West Lafayette, Indiana.

[9] Fabien A P P., "Watermarking Schemes Evaluation", IEEE Signal Processing Magazine, September 2000.

[10] Fernando P G and Juan R H., “A Tutorial on Digital Watermarking”, Department Tecnologıas Delas Comunicaciones, ETSI Telecom., Universidad de Vigo,Vigo, Spain.

[11] Frank Hartung, Martin Kutter, “Multimedia Watermarking Techniques”, Proceedings of the IEEE, Volume. 87, Issue. 7, July 1999.

[12] Gerhard C. L, Setyawan I,Reginald L L., "Watermarking Digital Image and Video Data", IEEE Signal Processing Magazine, September 2000.

[13] Gilani S A M., Skodras A N., “Watermarking by Multiresolution Hadamard transform”, Electronics Laboratory, University of Patras GR-26110 Patras, Greece.

[14] Hernandez, J R, Amado, M, Perez-Gonzalez, F., “DCT-domain watermarking techniques for still images”, IEEE Transactions on Image Processing, Volume. 9, Issue. 1, pp.55 – 68,January 2000.

[15] Ho A.T.S, Shen J, Chow A.K.K, Woon, J “Robust Digital Image-In-Image Watermarking Algorithm using the Fast Hadamard Transform”, Proceedings of

IEEE International Symposium on Circuits and Systems ,Volume 3, pp. 826-829,25-28 May 2003.

[16] Ho A.T.S, Shen J, SoonHie T, Kot A.C., "Digital Image-In-Image Watermarking for Copyright Protection of Satellite Images using the Fast Hadamard Transform", Proceedings of IEEE Symposium on Geoscience and Remote Sensing, Volume.6, pp.3311–3313, 2002.

[17] Huang J, Shi YQ, Shi, "Embedding Image Watermarks in DC Components", Proceedings of IEEE Transactions on Circuits and System for Video Technology, Volume. 10, Issue. 6, pp. 974-979, 2000.

[18] Ibrahim Nasir, Ying Weng, Jianmin Jiang, "A New Robust Watermarking Scheme for Color Image in Spatial Domain", School of Informatics, University of Bradford, UK.

[19] Kaewkamnerd N, Rao K.R., "Wavelet based image adaptive watermarking scheme" in IEE Electronics Letters, Volume-36,pp - 312-313, 17-February 2000.

[20] Kundur D, Hatzinakos D., "Towards Robust Logo Watermarking using Multiresolution Image Fusion," IEEE Transactions on Multimedia, Volume. 6, Issue. 1, pp.185-198, February 2004.

[21] Kundur. D., Hatzinakos, D., "Digital Watermarking using Multiresolution Wavelet Decomposition", Proceedings of IEEE International. Conference. On Acoustics, Speech and Signal Processing, Seattle, Washington, Volume. 5, pp. 2969-2972, May 1998.

[22] Liu Liang, Sun Qi, "A new SVD-DWT composite watermarking", Proceedings of 8th International conference on Siginal Processing, Volume. 4, pp.16-20, 2006.

[23] Petitcolas F A P., "Introduction to information hiding" in Information Techniques for Steganography and Digital Watermarking, Eds. Northwood, MA: Artec House, pp 1-11, December 1999.

[24] Potdar V M, Han S, Chang E.,"A Survey of Digital Image Watermarking Techniques" Proceedings of IEEE conference on Industrial Informatics, School of Inf. Syst., Curtin Univ. of Technol., Perth, WA, Australia.

[25] Saraju P. Mohanty., "Digital Watermarking : A Tutorial Review", Dept of Comp Sc and Engineering, Unversity of South Florida, Tampa, FL 33620.

[26]Saryazdi S, Hossein N P., "A Blind Digital Watermark in Hadamard Domain", Proceedings of World Academy of Science, Engineering and Technology, Volume. 3, January 2005.

[27] Solachidis, V & Pitas., "Circularly Symmetric Watermark Embedding in 2-D DFT Domain", in IEEE Transactions on Image Processing, Volume. 10, Issue. 11, pp.1741-1753.

[28] Tao B, Dickinson B, "Adaptive Watermarking in DCT Domain", Proceedings of. IEEE International Conference on Acoustics, Speech, and Signal Processing, Volume. 4, pp. 1985-2988, 1997.

[29] Tewfik A.H., "Digital Watermarking", in IEEE Signal Processing Magazine, Volume. 17, pp.17-88, September 2000.

[30] Tirkel A Z,van Schyndel R G,Osborne C F.,"Two-Dimensional Digital Watermark", Scientific Technology, P.O.Box 3018, Dendy Brighton, 3186, Australia.

[31] Xie, L, Boncelet, G, Acre G.R., "Wavelet transform based watermarking for digital images", in Optics Express, Volume. 3, Issue. 12, December 1998.

[32] Xinzhong Zhu, Jianmin Zhao and Huiying Xu, "A Digital Watermarking Algorithm and Implementation Based on Improved SVD", Proceedings of IEEE 18th International Conference on Pattern Recognition (ICPR'06), 2006.

BIBLIOGRAPHY

[1] Anil K Jain, "Fundamentals of Digital Image Processing", Prentice-Hall of India, 2000.

[2] Chun-Shien Lu, "Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property", Idea Group Publishing, 2005.

[3] Ian T. Young, Jan J. Gerbrands, Lucas J. van Vliet "Fundamental of Image Processing" , The Netherlands at the Delft University of Technology, 1998.

[4] Juergen Seitz, "Digital Watermarking for Digital Media", Infromation Science Publishing, 2004.

[5] Michael Arnold, Martin Schmucker and Stephen D.Wolthusen.,"Techniques and Applications of Digital Watermarking and Content protection", Artech House, Boston, London -2003.

[6] Stefan Katzenbeisser, Fabien A. P. Petitcolas, "Information Hiding Techniques for Steganography and Digital Watermarking" , Artech House, 2000.