Efficient Techniques for Digital Watermarking
S.R. Jayapriya¹ P. Narendran²
¹Research Scholar ²HOD
¹,²Department of Computer Science & Engineering
¹,²Gobi Arts and Science College, Gobi

Abstract— Digital watermarking is a pattern of bits inserted into a digital image, audio or video file that identifies the file's copyright information (author, rights, etc.). The purpose of digital watermarks is to provide information such as copyright protection, source tracking, hidden communication, broadcast tracking for intellectual property that is in digital format. Digital watermarking analysis has two different categories of watermarks, (i) sturdy and (ii) fragile. Sturdy watermarks area unit is designed to be detected even if one tries to get rid of them. Fragile watermarks area unit used for authentication functions and area unit is capable of sleuthing even minute changes of the watermarked content. Digital watermarks are designed to be completely invisible, or in the case of audio clips, inaudible. Moreover, the actual bits representing the watermark must be scattered throughout the file in such a way that they cannot be identified and manipulated. And finally, the digital watermark must be robust enough so that it can withstand normal changes to the file, such as reductions from lossy compression algorithms. The proposed method is quantization index modulation (QIM).

Key words: Watermarking, Robust, Quantization index modulation (QIM)

I. INTRODUCTION
A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as an audio, video or image data. It is typically used to identify ownership of the copyright of such signal[4]. "Watermarking" is the process of hiding digital information in a carrier signal. The hidden information should not need to, contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal. It is prominently used for tracing copyright infringements and for bank not authentication.

The digital watermarks is only perceptible under certain conditions, i.e. after using some algorithm, and imperceptible otherwise. A digital watermark that distorts the carrier signal in a way that it becomes perceivable, is of use[3]. Traditional watermarks may be applied to visible media (like images or video), where as in digital watermarking, the signal may be audio, pictures, video, texts or 3D models. A signal may carry several different watermarks at the same time. Unlike metadata that is added to the carrier signal, a digital watermark does not change the size of the carrier signal. These are the examples to the watermark overlay on an image.

The needed properties of a digital watermark depend on the use case in which it is applied. For marking media files with copyright information, a digital watermark has to be rather robust against modifications that can be applied to the carrier signal[5]. Instead, if integrity has to be ensured, a fragile watermark would be applied.

Both steganography and digital watermarking employ steganographic techniques to embed data covertly in noisy signals. But whereas steganography aims for imperceptibility to human senses, digital watermarking tries to control the robustness as top priority. A digital copy of data is the same as the original. Digital watermarking is a passive protection tool. It just marks data, but does not degrade it or control access to the data.

One application of digital watermarking is source tracking. A watermark is embedded into a digital signal at each point of distribution[1]. If a copy of the work is found later, the watermark may be retrieved from the copy if the source of the distribution is known. This technique reportedly has been used to detect the source of illegally copied movies.

II. DIGITAL WATERMARKING LIFECYCLE

General digital watermark life cycle phases with embedding, attacking and detection and retrieval functions.

The information to be embedded in a signal is called a digital watermark, although in some contexts, the phrase digital watermark means the difference between the watermarked signal and the cover signal. The signal where the watermark is to be embedded is called the host signal[8].

A watermarking system is usually divided into three distinct steps viz., embedding, attack, and detection. In embedding, an algorithm accepts the host and the data to be embedded, and produces a watermarked signal.

The watermarked digital signal is transmitted or stored, to be transmitted to another person. If this person makes a modification[3], this is called an attack. The modification may not be malicious, the term attack arises from copyright protection application. Third parties may attempt to remove the digital watermark through modification. There are many possible modifications. For example, lossy compression of the data (in which resolution is diminished), cropping an image or video, or intentionally adding noise.

Detection (often called extraction) is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. The signal was unmodified during transmission. The watermark still is present and it may be extracted. In robust digital watermarking applications, the extraction algorithm should be able to produce the watermark correctly[1], even if the modifications were strong. In fragile digital watermarking, the extraction algorithm should fail if any change is made to the signal.

A watermark is an identifying image or pattern in paper that appears as various shades of lightness/darkness when viewed by transmitted light (or when viewed by reflected light, atop a dark background)[9], caused by...
thickmess or density variations in the paper. Watermarks have been used on postage stamps, currency, and other government documents to discourage counterfeiting[7]. There are two main ways of producing watermarks. The dandy roll process, and the more complex cylinder mould process.

III. RELATED WORK

The watermarking embeds possession of data in digital content. Watermark describes data that may be accustomed to prove the possession of electronic information service. Here the embedding is hidden that the presence of watermarking is invisible to the user. The planned approach permits us to, with success, mix the secure embedding of shopper aspect with the superior hardiness of aware embedding techniques, providing a replacement powerful tool for the secure distribution of prime quality multimedia system contents[2]. Open problems within the planned framework to be addressed within the future analysis concern the necessity of upper security and also the compression overhead. Shopper aspect watermark embedding systems are planned as a doable resolution for the copyright protection in large-scale content distribution environments.

Digital audio, video, images, and documents are flying through computer network to their individual owners. sadly, on the manner, people might choose to intervene and take this content for themselves. Digital watermarking and steganography technology greatly reduces the instances of this by limiting or eliminating the power of third parties to decipher, the content that he has taken. The numerous techniques of digital watermarking (embedding a code) and steganography (hiding information) still evolve as applications that necessitate do an equivalent[6]. The authors of this second edition offer an update on the framework for applying these techniques that they provided researchers and professionals within the initial well-received edition. Steganography and steganalysis are extra to a strong treatment of digital watermarking, as several in every field analysis and subsume the other. New material includes watermarking with facet data, QIM, and dirty-paper codes.

A category of embedding ways referred to as quantisation index modulation(QIM) . These ways, and low-complexity realizations of them referred to as dither modulation[4]. Square measure incontrovertibly higher than each antecedently projected linear ways of unfold spectrum and nonlinear ways of low-bits modulation against square-error distortion-constrained intentional attacks. Gaussian host signal and additive colored gaussian noise attacks. These results imply associate degree data embedding capability of regarding 1/3 b/s of embedded digital rate for each hertz of host signal information measure and each decibel come by received host signal quality. We tend to see that QIM ways succeed performance at intervals 6 decibel of capability, introduce a kind of post processing we ask as distortion compensation that, once combined with QIM, permits capability to be achieved. Additionally, we tend to associate degreëalysed that distortion-compensated QIM is an optimum embedding strategy against some necessary categories of intentional attacks furthermore. Finally. We tend to report simulation results that demonstrate the performance of dither modulation realizations which will be enforced with solely some adders and scalar quantizers.

Analysis the performance of spread-transform dither modulation (ST-DM). Watermarking within the presence of two vital categories of non additive attacks, like the gain attack and noise addition, and also the division attack area unit evaluated. The analysis is developed underneath the idea that the host options are independent and identically distributed gaussian random variables, which a minimum distance criterion is employed to rewrite the hidden info. The theoretical bit-error possibilities square measure derived in closed kind, therefore permitting to evaluate the impact of the though-about attacks on the watermark at a theoretical level[3]. The analysis is valid by means that of intensive the simulations. Additionally the validation of the theoretical analysis, the simulations allowable to abandon the hypothesis of usually distributed host options, in favor of additional realistic models adopting a Laplacian or a generalized gaussian likelihood density operate. The overall results of our analysis are that the wonderful performance of ST-DM area unit confirmed all told cases with the sole noticeable exception of the gain attack.

IV. PROPOSED SYSTEM

The projected system choose a strong parameter to embed knowledge. In this projected formula, a data point amount is chosen and then parameter get an unique strong lossless image. The knowledge concealment technique employs a applied mathematics as a parameter for knowledge embedding, so with success avoiding salt-pepper noise. Once somebody tries to form associate degree unauthorized copy of the transmission content. The duplicate copy also will have a novel image to text watermarking embedded in every bit of the transmission contents. If the image to text watermarking pictures it distributed to the client it is simple to seek out. The one is creating the pirated copies whether or not the client or the content supplier.

V. CONCLUSION

Multimedia security is extraordinarily important concern for the net technology due to the ease of the duplication. Distribution and manipulation of the multimedia system information. The digital watermarking could be a field [info]of data[info] knowledge concealment that hide the crucial infomation. The original information for cover criminal duplication and distribution of multimedia system information. This present digital image watermarking techniques.

The results of various digital image watermarking techniques are compared on the premise of outputs. In the digital watermarking the key data are ingrained into the first information for protecting the possession rights of the multimedia system information. The image watermarking techniques may divide on the premise of domain like abstraction domain or rework domain or on the premise of wavelets. The abstraction domain techniques directly work on the pixels and also the frequency domain works on the rework coefficients of the image. This survey elaborates the foremost vital methods of abstraction domain and rework.
domain and focuses the deserves and demerits of those techniques.

REFERENCES


