International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353 Volume 4 Issue 1 –DECEMBER 2013.

Secure Spread Spectrum Technique for Data Hiding using Image watermarking

G.Kavitha [#1], C.Sasikumar [*2]

[#] *Head of the Department, Excel Engineering College, Komarapalayam, TamilNadu, India.*

[*] *Assistant Professor, Excel Engineering College, Komarapalayam, TamilNadu, India.*

[1]hod_cse_eec@yahoo.in

Abstract: Watermarking is the process of stereography or embedding process. It is mainly proposed for copyright protection, data security, and data hiding and conveys other information etc. The Watermarking project is achieved by spread spectrum technique. The advantage of this technique is providing security, avoid host interferences and improve the decoder performance. Embedding data to the video frames is achieved by following steps. At first step, by using string technique data is watermarked to an image. Watermarking object is retrieved by using technique without any data loss. DWT domain provides decomposition in an object, the proposed system results provide better Peak Signal to Noise Ratio (PSNR) and Bit Error Rate (BER).

Keywords: Digital image processing, video watermarking, data hiding, MATLAB

I. INTRODUCTION

Information hiding can be mainly divided into three processes cryptography, stenography and watermarks. Cryptography is the process of converting information to an unintelligible form so that only the authorized person with the key can decipher it. As many advances were made in the field of communication it became rather simple to decrypt a cipher text. Hence more sophisticated methods were designed to offer better security than what cryptography could offer. This led to the discovery of stenography and watermarking. Stenography is the process of hiding information over a cover object such that the hidden information cannot be perceived by the user. Thus even the existence of secret information is not known to the attacker. Watermarking is closely related to stenography, but in watermarking the hidden information is usually related to the cover object. Hence it is mainly used for copyright protection and owner authentication. The watermarking system is usually divided into three distinct steps, embedding, attack and detection. In embedding, an algorithm accepts the host and the data to be embedded and produces a watermarked signal. The watermarked signal is then transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. There are many possible attacks. Detection is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was not modified during transmission, then the watermark is still present and it can be extracted. If the signal is copied, then the information is also carried in the copy. The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data, it is carried with the signal itself.

The original image and the desired watermark are embedded using one of the various schemes that are currently available. The obtained watermarked image is passed through a decoder in which usually a reverse process to that employed during the embedding stage is applied to retrieve the watermark. The different techniques differ in the way in which it embeds the watermark on to the cover object. A secret key is used during the embedding and the extraction process in order to prevent illegal access to the watermark.

A. Requirements:

The major requirements of digital watermarking are:

a)Transparency:

The embedded watermark should not degrade the original image. If visible distortions are introduced in the image, it creates suspicion and makes life ease for the attacker .It also degrades the commercial value of the image.

b) Robustness:

This is by far the most important requirement of a watermark. There are various attacks, unintentional (cropping, compression, scaling) and unintentional attacks which are aimed at destroying the watermark. So, the embedded watermark should be such that it is invariant to various such attacks.

c) Capacity or Data Load:

This quantity describes the maximum amount of data that can be embedded into the image to ensure proper retrieval of the water during extraction.

B. Watermark Classification

There are several criteria how watermarks for images or video sequencescan be classified.

Watermarking techniques can be classified into spatial or frequency domain by place of application. Spatial domain watermarking is performed by modifying values of pixel color samples of a video frame such as in [2] whereas watermarks of frequency domain techniques are applied to coefficients obtained as the result of a frequency transform of either a whole frame or single block-shaped regions of a frame. Discrete Fourier Transform watermarking using this transform is presented in [3] and Discrete Wavelet Transform in [4] or [5] belong among whole-frame frequency transforms. The representative of the block frequency transform is Discrete Cosine Transform in [6]. Classification into these groups is according to the way how the transforms are usually used in practice .Video sequences compressed by modern techniques offer another type of domain, motion vectors. Watermarking in this domain slightly alters length and direction of motion vectors as in [7].Further, watermarks for video sequences can be classified by the range of application e.g. hidden information carried by a watermark can be spread over all frames of the video sequence, then the whole sequence is necessary to retrieve that information, or each frame contains watermark with the same information, then only a single frame should be enough In one frame, one single element of the watermark can be embedded into one pixel, into a block of pixels or even into the whole frame.

C. Application of watermarking

A popular application of watermarking techniques is to provide a proof of ownership of digital data by embedding copyright statements into video or image digital products.

Other applications include:

Automatic monitoring and tracking of copy-write material on WEB. (For example, a robot searches the Web for marked material and thereby identifies potential illegal issues.)

Automatic audit of radio transmissions: (A robot can “listen” to a radio station and look for marks, which indicate that a particular piece of music, or advertisement , has been broadcast.)

Data augmentation - to add information for the benefit of the public

Fingerprinting applications (in order to distinguish distributed data)

Actually, watermarking has recently emerged as the leading technology to solve the above very important problems. All kind of data can be watermarked: audio, images, video, formatted text, 3D models, and model animation parameters

II. QUANTIZATION TECHNIQUES

Fernando Pérez-González, Carlos Mosquera, Mauro Barni and Andrea Abrardo proposed a novel quantization- based data-hiding method, called Rational Dither Modulation (RDM) [1][12], is presented. This method retains most of the simplicity of the conventional dither modulation (DM) scheme, which is largely vulnerable to amplitude scaling and modifies it in such a way that the result becomes invariant to gain attacks. RDM is based on using again-invariant adaptive quantization step-size at both embedder and decoder. This causes the watermarked signal to be asymptotically stationary. Mathematical tools are used to determine the stationary probability density function, which is later used to assess the performance of RDM in Gaussian channels. RDM is compared with improved spread-spectrum methods, showing that the former can achieve much higher rates for the same bit error probability. Finally, a broader class of methods, that extends gain-in variance to quantization index modulation (QIM) methods, is also presented. The current RDM proposal has proven its merits in a highly theoretical context, which is largely independent of the host nature; needless to say, a considerable amount of work is necessary to tune RDM to the demands of practical applications. For instance, our assumption of a stationary host is far from holding with real signals. A partial relief would be to pseudo randomly permuting the host samples to create a “pseudo- stationary” signal, but in turn, this may affect RDM’s resilience to slow-varying gains. Other open implementation issues that need be taken into consideration include the use of varying embedding strengths, practical effects of the embedding PAR, the selection of the quantization step, and the initialization of the function Besides the practical implementation of RDM with multimedia signals, ongoing research covers the design of the function controlling the step size, with the possible inclusion of weighted norms, the combination of RDM with distortion compensation and channel coding, and the adaptation of RDM to deal with faster gain variations.

Brian Chenand Gregory W. Wornell, proposed a new method to avoid the problem of embedding one signal (e.g., a digital watermark), within another “host” signal to form a third, “composite” signal The embedding is designed to achieve efficient tradeoffs among the three conflicting goals of maximizing information-embedding rate, minimizing distortion between

the host signal and composite signal, and maximizing the robustness of the embedding, introduce new classes of embedding methods, termed quantization index modulation (QIM) and distortion-compensated QIM (DC-QIM), and develop convenient realizations in the form of what we refer to as dither modulation. Using deterministic models to evaluate digital watermarking methods, we show that QIM is “provably good” against arbitrary bounded and fully informed attacks, which arise in several copyright applications, and in particular, it achieves provably better rate distortion–robustness tradeoffs than currently popular spread-

spectrum and low-bit(s) modulation methods of probabilistic models, DC-QIM is optimal (capacity-achieving) and regular QIM is near-optimal. These include both additive white Gaussian noise (AWGN) channels, which may be good models for hybrid transmission applications such as digital audio broadcasting, and mean-square-error-constrained attack channels that model private-key watermarking applications.

III. SPREAD SPECTRUM SCHEMES

Spread Spectrum schemes represent an early type of embedding method. It adds a sequence of pseudo-random signals into the host signals to form the watermarked data. According to how the watermark is added into the host contents, the spread spectrum schemes can be further subdivided into the additive and multiplicative spread spectrum (ASS and MSS) schemes. The signals are usually embedded into the perceptually important components of the host image to achieve a balance of perceptual quality and robustness. At the detector, the original image should be available to cancel the watermarked image to extract the embedded signals. The extracted signals are then correlated with a predefined pattern for validation. The detection that requires the original data is called private detection.

For many prospective applications, this requirement is sometimes quite astringent. Later, Piva andZeng designed [10][11] the blind detection techniques which require no presence of the original hosts. The blind detection employs the statistical inference to differentiate between the unwater marked and the watermarked contents. In these blind schemes, the original work is taken as the noise interfering with the watermarking detection. The host interference should not be a problem if it is available at the detector or decoder. For many prospective applications, this is not the case. This situation can be further improved by designing a better embedded or an optimum detector or decoder. The first approach utilizes the host information at the embedded, whereas the second, it improves the performance of spread spectrum watermarking schemes by exploiting the probability distribution function (pdf) of the host signals at the detector or decoder.

Side-informed embedded

Cox model as the watermarking as communication with side information, and proposed to utilize the host information in the embedding process. The idea was that instead of treating the cover data as noise added to the embedded signals, it could be taken as side information to improve both the fidelity and the detection rate by means of an appropriate perceptual mask and the knowledge of the detector. First Approach: perceptual models.

Using a global embedding strength results in the perceptible local distortion. Thus many authors proposed to locally bound the maximum embedding strength by the Human Perceptual Systems (HPS) to achieve the maximum allowable perceptual distortion and robustness Podilchuk and Zeng utilized the Watson's perceptual model to embed the perceptually-shaped signals into the host contents.

The Watson's model, initially designed for image compression, includes three Major perceptual functions namely frequency, luminance and contrast masking. Tuned with this model, the image quality is much improved, especially at the smooth regions of the images that are more sensitive to the image manipulations. Since the embedding strength can be locally bounded to achieve a distortion of one Just Noticeable Difference (JND) level, a higher robustness can also be achieved a acceptable image quality. The idea of employing perceptual models is further extended to the video watermarking. In the authors presented a perceptual model in the DFT domain. In addition to the masking criterion, the model also discriminates the different perceptual effects of edge and texture.

The model investigated in exploits the temporal and the frequency masking to guarantee that the embedded watermark is inaudible and robust. Similar ideas of using perceptual models to improve both the perceptual quality and the robustness. Second approach: side-informed techniques with the knowledge of the structure of the detector (a kind of reverse engineering to compute the desired embedding signals.) Based on Cox's frame work aside-informed embedder is designed according to a specified criterion, such as maximizing the correlation coefficient or maximizing the robustness.

Since both the correlation coefficient and the robustness are related to the host contents, the embedded signals thus depend on the host contents. In order to achieve the best perceptual quality at a fixed robustness, Miller et al. presented an iterative embedding algorithm that builds the watermark by adding perceptually shaped components until the desired robustness is achieved. Similar ideas are also formulated however; these side-informed schemes do not handle the important issue of how to insert the watermark to minimize the error rate at a fixed distortion level. Improved Spread Spectrum (ISS) scheme proposed also exploits the knowledge of host contents by projecting them into the watermark, and this projected host interference is then compensated in the embedding process. The authors claimed that the performance measured in probabilities of errors could be improved by tens of magnitudes. This is not strange since ISS is quantization scheme with only two quantizers. The second approach succeeds is removing (or partially removing) the host interference and thus improves the system's performance.

Comparison of the above two approaches: The embedder of the first approach does not require the knowledge of the detector's structure, whereas the second instance, Miller's maximum robustness assumes that the detection statistic is the correlation coefficient. For ISS, the detector is a simple linear correlator. The second approach excels the first performance since it offers a property of host interference rejection. For instance, ISS can have a complete rejection of the host interference. It also due to the host interference property and it is difficult to implement the perceptual analysis for the second approach since the embedded signal relies on the summary of the host features.

Informed detector:

The detector has to be informed the host pdf (and the embedding strengths for some cases, i.e., optimum detectors.) Hernande designed an optimum detector for ASS watermarking in the Discrete Cosine Transform (DCT) domain. Their detector exploits the fact that the host's low- and mid-frequency DCT coefficients can be better model by Generalized Gaussian Distributions (GGD).Briassouli exploited the fact that Cauchy pdf also gives a better approximation of the low- and mid-frequency DCT coefficients, and designed a locally optimum Cauchy nonlinear detector. According to their comparison of results, it is hard to say whether Cauchy model yields a better performance than GGD model.In truth, GGD models are much more popular modeling than DCT coefficients. For MSS, Oostveenand Barni modeled the magnitudes of Discrete Fourier Transform (DFT) coefficients through a Weibullpdf and investigated the optimum detection in the DFT domain. For multiplicative watermarking in the DCT domain, Cheng derived the structure of its optimum detector. In this paper, Cheng also derived a class of generalized correlators. Unlike the previous Universally Most Powerful (UMP) detectors, this class of detectors is derived from the Locally Optimal (LO) or Locally Most Powerful (LMP) tests. Recently, an optimum decoder for information hiding in the Laplacian Discrete Wavelet Transform (DWT) data was proposed. All the above optimum detectors are derived under the hypothesis that no attack is mounted on the host contents.

Wavelet-domain Domain Technologies

The new big standard has adopted a new technique, the wavelet transform. Though this standard has not been widely used yet, any new watermarking algorithm that intends to survive in the future should get along with it. Here come the watermarking schemes based on wavelet transform. The difference between different wavelet domain methods depends on the way the watermark is weighted. The reason for this is to reduce the presence of visual artifacts. The DWT (Discrete Wavelet Transform) separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components.

One of the many advantages over the wavelet transform is that that it is believed to more accurately model aspects of the HVS as compared to the FFT or DCT, Higher compression ratio Avoid blocking artifacts Allows good localization both in time and spatial frequency domain. Transformation of the whole image introduces inherent scaling This allows us to use higher energy watermarks in regions that the HVS is known to be less sensitive to, such as the high resolution detail bands {LH, HL, HH) Embedding.

IV. SECURE SPREAD SPECTRUM TECHNIQUE FOR DATA HIDING USING IMAGE WATERMARKING

In proposed system the data is hidden in to the image To achieve the better performance value we used 512x512 as a image size to hide the data. In this we can hide 32x32 sizes of data that data is hided in to any place of the input image. We can change the position easily it provide the better security. The proposed system has the following advantages it provide better decoder performance. we can use both color and gray level video to hide the dada. We can extract the low frequency component so for there is no loss in frequency component of the video it improves the clarity of the video. Spread spectrum technique is Resist intentional and unintentional interference .Can share the same frequency band with other users (multiple watermarks).Protect the privacy, due to the pseudo random code sequence. Haar transform is used to composition and decomposition Why Haar Wavelets? There are a wide variety of popular wavelet algorithms, including Daubechies wavelets, Mexican Hat wavelets and Marled wavelets. These wavelet algorithms have the advantage of better resolution for smoothly changing time series. But they have the disadvantage of being more expensive to calculate than the Haar wavelets. The higher resolution provided by these wavelets is not worth the cost for financial time series, which are characterized by jagged transitions. The Haar wavelet transform has a number of advantages: It is conceptually simple. It is fast. It is memory efficient, since it can be calculated in place without a temporary array. It is exactly reversible without the edge effects that are a problem with other wavelet transforms.

V. ALGORITHM

The algorithm of watermarks Embedding and decoding is given bellow.

Watermarks Embedding Algorithm

Step 1: Read the image
Step 2: Resize the frames to 512x512.
Step 3: Get the message.
Step 4: Convert it into decimal to binary.
Step 5: Create an empty window using zeros and replace the zeros with the converted binary value.
Step 6: Apply scrambling.
Step 7: Apply mean removal
Step 8: Embed the message into the image

Watermarks Decoding Algorithm

Step 11: Get the frame from watermarked image.
Step 12: Apply 2 level dwt.
Step 13: Apply sub band analysis.
Step 14: Apply descrambling.

Step 15: De embed the message from the image .

Step 16: Final display the message by converting it into binary to decimal.

VI. CONCLUSION

In this paper, we have introduced secure spread spectrum technique using video watermarking for data hiding it provide better PSNR value and minimum BER and improved decoder performance over the existing systems. The Haar transform has some limitations, which can be a problem with for some applications. In generating each of averages for the next level and each set of coefficients, the Haar transform performs an average and difference on a pair of values. Then the algorithm shifts over by two values and calculates another average and difference on the next pair. The high frequency coefficient spectrum should reflect all high frequency changes. The Haar window is only two elements wide. If a big change takes place from an even value to an odd value, the change will not be reflected in the high frequency coefficients. So Haar wavelet transform is not useful in compression and noise removal of audio signal processing. To further investigate the performance of the proposed system, experiments on a large data base of real images were demonstrated.

VII. REFERENCES

[1] Fernando Pérez-González, Carlos Mosquera, Mauro Barni, and Andrea Abrardo "Rational Dither Modulation: A High-Rate Data-Hiding Method Invariant to Gain Attacks "IEEE transactions on signal processing, vol. 53, no. 10, October 2005.

[2] R. Popa, "An analysis of steganographic techniques", The Politehnica University of Timisoara, Faculty of Automatics and Computers, Department Of Computer Scienceand SoftwareEngineering,Website:http://ad.informatik.unifreiburg.de/mitarbeiter/will/dlib_bookmarks/digital- watermarking/popa/popa.pdf, 1998.

[3] P. Vidyasagar, S. Han and E. Chang. "A survey of digital image watermarking techniques", 3rd IEEE International Conference on Industrial Informatics (INDIN 2005), edited by T. Dillon, X. Yu. And E. Chang, pp. 495-502, Perth, Western Australia, 2005.

[4] J. Dugelay and S. Roche, "A Survey of Current Watermarking Techniques" in Information Techniques for Steganography and Digital Watermarking, S.C. Katzenbeisser et al, Eds. Northwood, MA: Artec House, pp. 121-145, Dec. 1999.

[5] I. J. Cox, et al, "Digital watermarking and steganography" (Second Edition), Morgan Kaufmann, 2008.

[6] K. R. Rao and P. Yip, "Discrete Cosine Transform: Properties, Algorithms, Advantages, Applications", Academic Press, Massachusetts, 1990.

[7] Brian Chenand Gregory W. Wornell "Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding" IEEE transactions on signal processing 2001.

[8] T. C. Lin and C. M. Lin, "Wavelet based copyright protection scheme for digital images based on local features", Information Sciences: an International Journal, Vol. 179, Sept. 2009.

[9] Jidongzhong and shangtenghuang "An enhanced multiplicative spread spectrum watermarking scheme" IEEE transations on circuits and systems for viedo technology, vol 16, no.12, December 2006.

[10] Amir Valizadeh, and Z. Jane Wang,An "Improved Multiplicative Spread Spectrum Embedding Scheme for Data Hiding" IEEE transactions on information forensics and security, vol. 7, no. 4, august 2012.

[11] I.J. Cox, M.L. Miller, J.M.G. Linnartz and T. Kalker, "A Review of Watermarking Principles and Practices" in Digital Signal Processing for Multimedia Systems, K.K. Parhi and T. Nishitani, New York, Marcel Dekker, New York, pp. 461-482, 1999.s

[12] NimaKhademiKalantari and Seyed Mohammad Ahadi "A Logarithmic Quantization Index Modulation for Perceptually Better Data Hiding" IEEE transactions on image processing, vol. 19, no. 6, June 2010.