Volume: 5 Issue: 6 Pages: 2092-2095 (2014) ISSN : 0975-0290

New Image Watermarking scheme for Information Security

V. Lokeswara Reddy
Department of CSE, K.S.R.M. College of Engineering,Kadapa, A.P. (India)
Email: vl_reddy@yahoo.com
P. Asif Ahamad, P. Salman Khan, P. Vivekananda,
Department of CSE,K.S.R.M. College of Engineering,Kadapa, A.P. (India)
Email: asif.ahamad.p@gmail.com
patansalmankhan786@gmail.com
viwek.pantangee@gmail.com

---**ABSTRACT**---

Digital Watermarking is a technology that embeds information or copyright notices or other verification messages, in machine-readable form, within the content of a digital media file. Watermarks can either be visible or invisible. This technique is better than Digital Signatures and other methods because it does not increase overhead. Digital Watermarking describes methods and technologies that hide information, for example numbers or text, in digital media, such as images, video or audio. The embedding takes place by manipulating the content of the digital data.A digital watermark is a signal permanently embedded into digital data that can be detected or extracted later by means of computing operations in order to make assertions about the data. The watermark is hidden in the host data in such a way that it is inseparable from the data and so that it is resistant to many operations not degrading the host document. Thus by means of watermarking, the work is still accessible but permanently marked. In this new image watermarking scheme the embedding process is done by using Bit replacement technology, which stores multiple copies of the same data that is to be hidden in scrambled form in the cover image. Then, in the recovery process of watermarked image we use Common sense method to recover the closest information from the damaged copies of the data under attack.

Keywords -Cover image, secrete logo, Haar filter, DWT

1.INTRODUCTION

Recent study has witnessed the rapid development in information technologies that has given an extended and easy access to digital information. Along with several developments it leads to the problem of illegal copying and redistribution of digital media. As a result the integrity and confidentiality of the digital information has come under immense threat. The concept of an emerging technology, digital watermarking came in order to solve the problems related to the intellectual property of media. 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. Instead, if integrity has to be ensured, a fragile watermark would be applied. Both steganography and digital watermarking employ steganography 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.

Digital Watermarking is a technique which allows an individual to add hidden copyright notices or other verification messages or even classified information to digital media [1]. Watermarks can either be visible or invisible. Since 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 nor controls 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. In this system, we utilize the invisible technique. This is used in public information settings such as digital images libraries, museums, and art galleries and also in defense communication where information security is of prime importance. Watermark embedding utilizes two kinds of methods; one is in the spatial domain[6] and the other in the transform domain. In the spatial domain, the watermark is directly embedded into the image Pixels whereas in the frequency domain, the image is decomposed into blocks and then mapped into the transform domain.

2.PROPOSED SYSTEM

Our proposed methodology for data hiding does not follow the old LSB technique [4] because of its small limitations. We have developed a new digital watermarking scheme that uses several bits of the cover image starting from lower order to higher order to hide the information logo. Here we generally hide several sets of the same data forming the information logo into the cover image. So if some of the information is lost due to attack, we can still collect the remaining information from the cover image and can reconstruct the hidden information very closer to the original one.

Advantages:

1. As the number of position for hiding the several sets of the same data forming the information logo into the cover image increase the noise resistance gets increased.
2. We can recover the very closer information even though the image is attacked and lost some information.

After careful analysis the system has been identified to have the following steps:

1. Embedding of watermark into cover image.
2. Recovery of watermark from watermarked image without any attack.
3. Recovery of watermark from watermarked image under attacks.

1. Embedding of watermark into cover image:

Three sets of cover image along with three information logo are taken as input and watermarked image as result of embedding technique. The computed value of quality matrices are also given to find the image quality.

2. Recovery of watermark from watermarked image without any attack:

Primarily we have considered the communication is ideal and hence no external interference has been included. In practice in the real world scenario we have to consider the noise and which are being incorporated in present experiment into the sent watermarked image. There are chances of unauthorized users in reality where the watermarked image can also be easily altered by unauthorized access from unwanted users.

3. Recovery of watermark from watermarked image under attacks:

In watermarking terminology, an attack is any processing that may impair detection of the watermark or communication of the information conveyed by the watermark. The processed watermarked data is then called attacked data.

There are two kinds of watermark attacks: non-intentional attacks, such as compression of a legally obtained, watermarked image or video file, and intentional attacks, such as an attempt by a multimedia pirate to destroy the embedded information and prevent tracing of illegal copies of watermarked digital video. In present we have considered one attack.

METHODS:

Least Significant Bit Modification:

The well-known method of watermark embedding, would be to embed the watermark into the least-significant-bits of the cover object [2]. In this method, a smaller object may be embedded multiple times [3]. Even if most of these objects are lost due to performed attacks, a single detection of watermark would be success for this system.

LSB substitution however despite its simplicity brings a host of drawbacks. Although it may survive transformations such as cropping, any addition of noise or lossy compression is likely to defeat the watermark. An even better attack would be to simply set the LSB bits of each pixel to one fully defeating the watermark with negligible impact on the cover object. Furthermore, once the algorithm is discovered, the embedded watermark could be easily modified by an intermediate party.

An improvement on basic LSB substitution would be to use a pseudo-random number generator to determine the pixels to be used for embedding based on a given key [2]. Security of the watermark would be improved as the watermark could no longer be easily viewed by intermediate parties. The algorithm however would still be vulnerable to replacing the LSB's with a constant. Even in locations that were not used for watermarking bits, the impact of the substitution on the cover image would be negligible. LSB modification proves to be a simple and fairly powerful tool for stenography, however lacks the basic robustness that watermarking applications require.

Discrete Wavelet Transforms (DWT):

Another possible domain for watermark embedding is that of the wavelet domain. The DWT (Discrete Wavelet Transform) separates an image into a lower resolution approximation image Low-Low (LL) as well as horizontal High-Low (HL), vertical Low-High (LH) and diagonal High-High (HH) detail components. The process can then be repeated to computes multiple "scale" wavelet decomposition, as in the 2 scale wavelet transform shown below in figure [7].

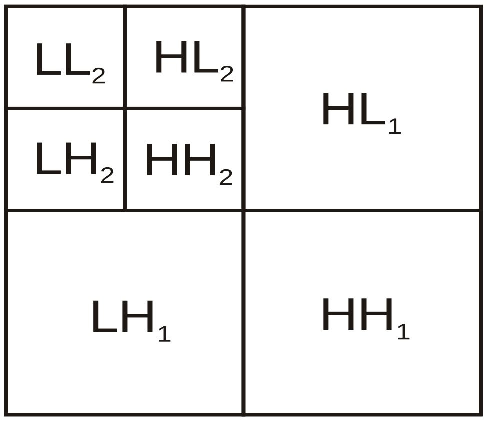

Figure Scale 2-Dimensional Discrete Wavelet Transform

One of the many advantages over the wavelet transform is that it is believed to more accurately model aspects of the HVS as compared to the DCT (Discrete Cosine Transforms). 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, and HH). Embedding watermarks in these regions allow us to increase the robustness of our watermark, at little to no additional impact on image quality.

One of the most straightforward techniques is to use a similar embedding technique to that used in the DCT, the embedding of a CDMA sequence in the detail bands according to the equation shown below in figure[6].

$$I_{W\,u,v} = \begin{cases} W_i + \alpha|W_i|x_i, & u,v \in HL, LH \\ W_i & u,v \in LL, HH \end{cases}$$

Common Sense Method:

To recover the image, if any attacks are performed on the image we just use common sense to choose the best pixel from multiple copies of retrieved pixels. If attacks are performed then some logos are damaged. Since we have multiple copies of hidden information, we compare the information with other pixel values and choose best similar pixels from the available pixels. The recovered information is practically not identifiable but the final derived logo is quite identifiable.

2.3Embedding/De-Embedding Process

In the proposed system, we put six copies of logo in the cover image. The positions for the logos are calculated using Haar technique of DWT.

LL	HL
LH	HH

Fig. Showing the four domains of the image

2.3.1 Embedding process:

In this embedding process,

Step 1: Cover image is selected such that multiple copies of information can be hidden in cover image.

Step 2: Then we apply Haar filter technique to divide the image into four sub domains.

Step 3: Then we mix the multiple copies of secret information in the cover image.

Step 4: To send this secret information to others, we send Watermarked image and secret keys.

Step 5: Secret keys are the height, width & pixel length.

2.3.2 Recovery process:

Step 1: Watermarked image is selected and then we apply algorithm to recover the image.

Step 2: Extract the embedded logo.

Step 3: Use common sense method to get the original hidden information.

3. EXPERIMENTAL WORK:

When the system is executed GUI (Graphical User Interface) is displayed. The snapshot of main window is shown below in figure 3. It shows the operations performed like choosing file, Haar filter technique, mixing image, recovering, adding noise.

Fig 3. Snap shot of Main Screen The snap shot of applying Haar filter technique is shown in figure 4.

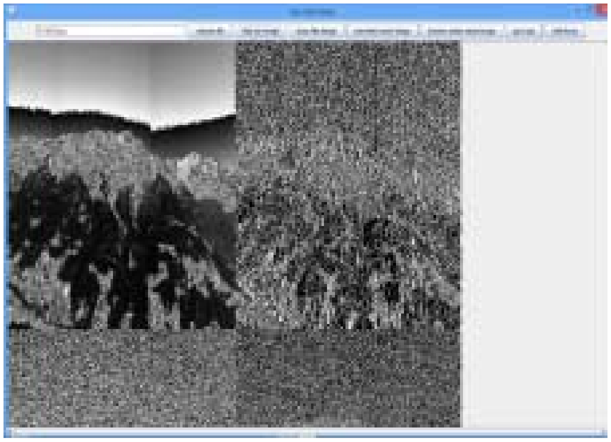

Fig 4. Haaf filter technique

The snapshot of Embedding window is shown in figure 5. In this, we are selecting a logo to hide in the cover image.

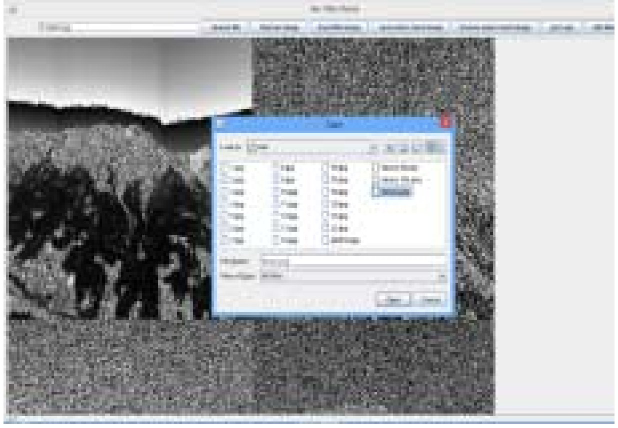

Fig 5. Selection of logo to embed into Cover image

The snap shot of cover image after adding noise or attack is shown in figure 6.

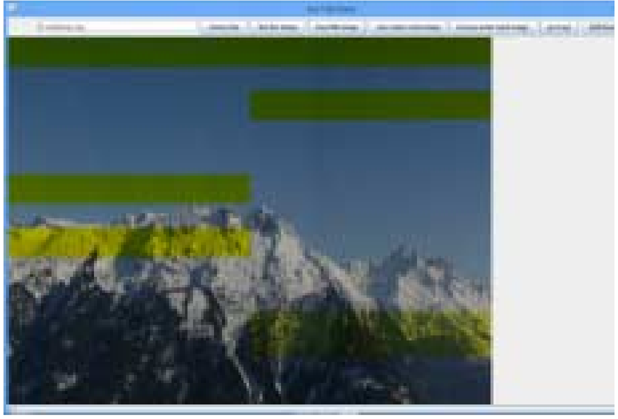

Fig 6. Showing image after adding noise or attack

The snap shot of recovered logo after adding noise on the Watermarked image is shown below.

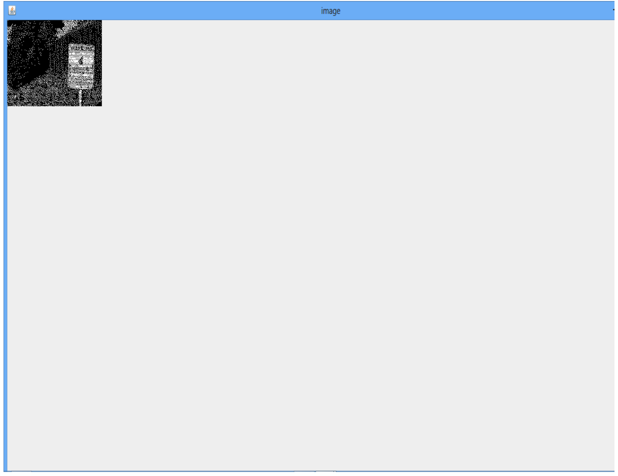

Fig 7. Recovered logo after attack

Conclusion:

The proposed algorithm aims at obtaining a solution to the several problems of digital communication and also for data hiding. It has been seen that the proposed algorithm is robust against 'salt and pepper' noise attack and also utilizes a private key which is required for the recovery of the hidden information and hence lending security to the algorithm.

It is also seen that the embedded information is successfully recovered from the watermarked image by using majority algorithm technique. The majority algorithm technique is very much efficient and a newer approach which is very unique and easy to understand.

Hence we can conclude by stating the fact that the proposed algorithm provides a method for secure communication and data hiding.

References:

1. Cox I. J., Miller M., Bloom J., 2002, "Digital Watermarking," Morgan Kaufmann Publishers.
2. Ling Na Hu Ling Ge Jiang, Blind Detection of LSB Watermarking at Low Embedding Rate in Grayscale Images. M. Celik, G. Sharma, E. Saber and A. Tekalp. Hierarchical watermarking for secure image authentication with localization. IEEE Trans. Image Process, 11(6):585–595, June2002.
3. D. Osborne, D. Abbott, M. Sorell, and D. Rogers. Multiple embedding using robust watermarks for wireless medical images. In IEEE Symposium on Electronics and Telecommunications, page section 13(34), Timisoara, Romania, Oct. 2004.
4. Koushik Pal, G. Ghosh and M. Bhattacharya (2012). A Novel Digital Image Watermarking Scheme for Data Security Using Bit Replacement and Majority Algorithm Technique, Watermarking - Volume 1, Dr. Mithun Das Gupta (Ed.), ISBN: 978-953-51-0618-0.
5. Langelaar, G.C., Setyawan, I. & Lagendijk, R.L. 2000, "Watermarking digital image and video data", IEEE Signal Processing Magazine, vol. 17, no. 5, pp. 20-46.
6. Rakhee Lakhera, Alka Gulati, Shital GuptaNovel Approach for Watermarking using Dual Watermarking Technique in Noisy Regions. ,IJCEM Vol. 15 Issue 5, September 2012 ISSN (Online): 2230-7893.
7. Anubha Aggarwal, Ramnik Singh,International Journal of Engineering Trends and Technology (IJETT) – Volume 9 Number 5 - Mar 2014