International Journal of Scientific Research and Modern Education (IJSRME)
ISSN (Online): 2455 – 5630
(www.rdmodernresearch.com) Volume I, Issue I, 2016

LOSSLESS VISIBLE WATERMARKING

K. Jayagowri* & K. Ramamoorthy**
* PG Scholar, Department of Master of Computer Applications, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu
** Assistant Professor, Department of Master of Computer Applications, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu

Abstract:

Compressive sensing data watermarking makes it possible to acquire images of objects concealed underneath clothing by measuring the radiometric temperatures of different objects on a human subject. The goal of the work is to automatically detect and segment concealed objects in broadband 0.1 −1THz images. Standard segmentation algorithms are unable to segment or detect concealed objects. A novel approach relies on two stages. First, the remove the noise from the image using the anisotropic diffusion algorithm and then detect the boundaries of the concealed objects. Next using a mixture of Gaussian densities model the distribution of the temperature inside the image. Curves are evolved along the is contours of the image to identify the concealed objects. When compared with two state-of-the-art segmentation methods. Both methods fail to identify the concealed objects, while the method accurately detected the objects. In addition, the approach was more accurate than a state-of-the-art supervised image segmentation algorithm that required that the concealed objects be already identified. Also the approach is completely unsupervised and extremely fast.

Index Terms: Reversible Water Rmarking, Data Recovery, Data Quality, Robuetness & Numerical Data

1. Introduction:

Digital watermarking is the process of embedding information into a digital signal in a way that is difficult to remove. The term is derived from a process used in the production of bearing a watermark for visible identification. In digital watermarking, the signal may be audio, pictures, or video. If the signal is copied, then the information also is carried in the copy. A signal may carry several different watermarks at the same time. In visible digital watermarking, the information is visible in the picture or video. Typically, the information is text or a logo, which identifies the owner of the media. The image on the right has a visible watermark. When a television broadcaster adds its logo to the corner of transmitted video, this also is a visible watermark. In invisible digital watermarking, information is added as digital data to audio, picture, or video, but it cannot be perceived as such (although it may be possible to detect that some amount of information is hidden in the signal). The watermark may be intended for widespread use and thus, is made easy to retrieve or, it may be a form of Steganography, where a party communicates a secret message embedded in the digital signal. In either case, as in visible watermarking, the objective is to attach ownership or other descriptive information to the signal in a way that is difficult to remove. It also is possible to use hidden embedded information as a means of covert communication between individuals.

One application of watermarking is in copyright protection systems, which are intended to prevent or deter unauthorized copying of digital media. In this use, a copy device retrieves the watermark from the signal before making a copy; the device makes a decision whether to copy or not, depending on the contents of the watermark. Another application is in source tracing. A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later, then the watermark may be retrieved from the copy and the source of the distribution is known. This technique reportedly has been used to detect the source of illegally copied movies. Annotation of digital photographs with descriptive information is another application of invisible watermarking. While some file formats for digital media may contain additional information called metadata, digital watermarking is distinctive in that the data is carried right in the signal. 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. A 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.

Then the watermarked digital signal is transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. While the modification may not be malicious, the term attack arises from copyright protection application, where pirates 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. If the signal was unmodified during transmission, then 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, even if the modifications were strong. In fragile digital watermarking, the extraction algorithm should fail if any change is made to the signal.

2. Related Works:

Most of the existing works on VM provisioning and dynamic resource allocation for web-based systems can be classified into two main categories: Plan-based approaches and control theoretic approaches. Plan-based approaches can be further classified into workload prediction approaches and performance dynamics model approaches. One common characteristic of all of these existing works is that they do not use shared hosting. Another common characteristic is that they only provide a server-level scaling mechanism. Whereas, our proposed approach for web applications [1] also provides a separate mechanism for scaling of individual web applications. There are currently only a few approaches for cloud-based distributed video transcending. However, they do not address VM provisioning problem for on-demand video transcoding. Server consolidation approaches, such as [5], dynamically reallocate VMs to physical nodes with the aim of reducing total number of required nodes. However, in the context of cost-efficient VM provisioning from an IaaS cloud, we require a different type of server consolidation. It should periodically migrate all active web applications and user sessions from the least load under-utilized VM stoother VMs. Thus, releasing the least loaded VMs for termination. Therefore, our goal is to reduce number of provisioned VMs and their renting durations, rather than reducing number of physical nodes. Admission control approaches, such as aim to prevent server overloading under high load situations. One common characteristic of these traditional approaches, except is that they make decisions only on acceptance or rejection of incoming user load. The approach in [4] has its own disadvantages. The discount-charge model requires additional web pages to be included in the web application and it is only effective for e-commerce web sites when more users place orders. In the context of cloud computing, it may also be possible to defer the incoming load until some new VMs are provisioned or some existing VMs become less loaded. Therefore, there is an opportunity to develop an admission control mechanism, which may choose between using an existing VM or provisioning a new VM for accommodating new incoming load [2], [3].

3. Proposed Work:

The main problem that we intend to tackle is cost-efficient VM provisioning with augmented server consolidation and overload control on provisioned VMs. We seek solutions for multi-tier web applications and on-demand video transcoding. Although there are many similarities between VM provisioning for web applications and VM provisioning for video transcoding, each one of them also has its own challenges. In this section, we present the proposed approach while providing a brief overview of some of the most important challenges that it addresses. We propose a cost-efficient VM provisioning approach for multi-tier web applications [1] and on-demand video transcoding [3]. Moreover, for preventing servers from becoming overloaded, the VM provisioning approach is augmented with an admission control mechanism [2], [3]. Similarly, the underutilization of VMs is minimized by providing a VM consolidation mechanism.

VM Provisioning Delay In practice, it takes a few minutes to provision a VM from an IaaS provider [1]. Due to the inevitable VM provisioning delay, handling of a sudden spike in the incoming user load becomes a challenge. Some of the strategies that we use to overcome this drawback of public IaaS clouds include provisioning multiple VMs at a time [1], using additional VM capacity [1], and using load prediction to provision proactively [3].

4. Module:

- ✓ Authentication Module
- ✓ Access service
- ✓ Creating new VM using VMM
- ✓ Updating VM details to local agent
- ✓ Schedule the VM from local agent
- ✓ View All Reports from PM
- ✓ Buy new VM

Authentication Module: The user authentication module is to check whether the authorized user is logged in this authentication process is verify the user name and password is valid. Before logged in one time registration is mandatory. In this module has been followed the Register page all fields fill into the mandatory. And we will enter into user name and password servers as regular log in confidential.

Access Service: This module the user going to access the services from the service provider. Here the register users only access the service. User access service will be updated to the local agent the agent only getting the from accessing service user. And updated to the PM at the time of access service.

Creating New VM Using VMM: This module will use ti creating new VM for the user access the services it created by the VM Monitor. VM does not create VM without use of all VM here any VM will free means the VMM allocate the service the free VM. Here all the VM monitor by the VMM.

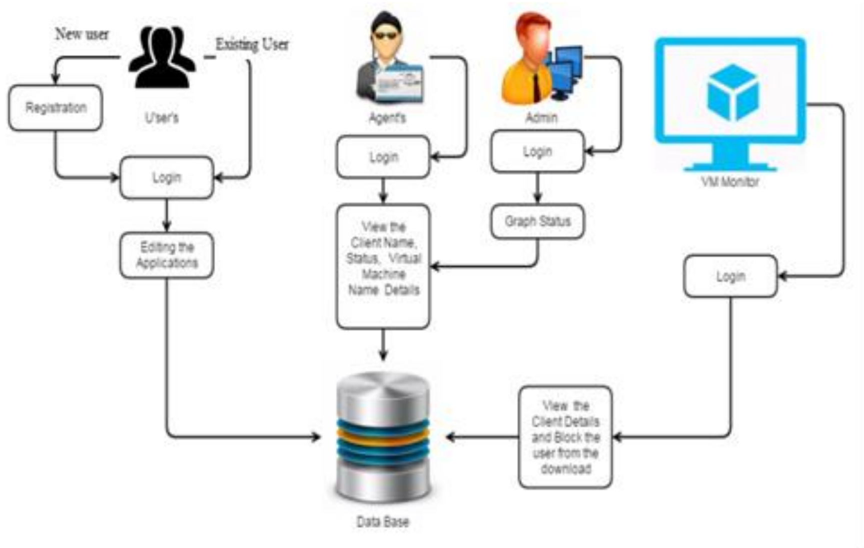
Updating VM Details to Local Agent: This module all the VM details like (Access service, free VM, load of the VM etc.,) updated to the local agent. At the same time the local agent update the VM details to the VM Monitor, here the VMM easily find the free VM and free services.

Schedule the VM From Local Agent: Here this module local agent will allocate the services to the VM, VM always will get the details and services from the local agent, here the local agent will get the the service information from the VM Monitor, and local agent also update the service details to the VM Monitor.

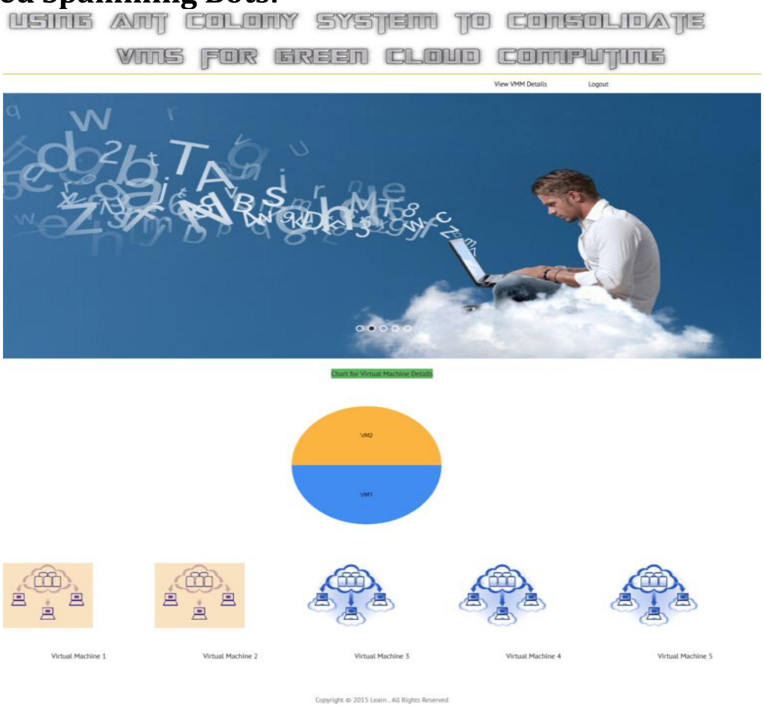
View All Reports from PM: In this module the PM (VM Monitor) will collect all the details from the local agent and also view over the entire VM load and allocated service details, here the VM Monitor will get the pie chart report about the VM and service details.

Buy New VM: In this module the VM monitor need any new VM they buy the new VM system at the time of all VM will busy, here the VM Monitor only buy the new VM. Before that the VM Monitor will check all the VM details.

5. System Architecture:



6. Network Based Spamming Bots:



7. Conclusion:

In this paper, we presented a novel dynamic Virtual Machine (VM) consolidation approach called Ant Colony System based VM Consolidation. It reduces the energy consumption of data centers by consolidating VM into a reduced number of active Physical Machines while preserving Quality of Service requirements. Since the VM consolidation problem is strictly we used the Ant Colony System (ACS) the main challenge is to reduce energy consumption of data centers while satisfying Quality of Service requirements. In this paper, we present distributed system architecture to perform dynamic VM consolidation to reduce energy consumption of cloud data centers while maintaining the desired Quality of Service.

8. References:

1. Ashraf, B. Byholm, J. Lehtinen, and I. Porres, "Feedback control algorithms to deploy and scale multiple web applications per virtual machine," 38th Euromicro Conference on Software Engineering and Advanced Applications, September 2012.
2. A. Vetro, C. Christopoulos, and H. Sun, "Video transcoding architectures and techniques: an overview," Signal Processing Magazine, IEEE, vol. 20, no. 2, pp. 18 – 29, mar 2003.
3. Buyya R, Yeo CS, Venugopal S, Broberg J, Brandic I. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems 2009; 25(6):599–616.
4. Amazon Elastic Compute Cloud (EC2). Available at: http://www.amazon.com /ec2 / [18 April 2010].
5. Chappell D. Introducing the Azure services platform. White Paper, October 2008