ISSN 2278-3083

International Journal of Science and Applied Information Technology (IJSAIT), Vol. 3 , No.4, Pages :72 - 74 (2014)
Special Issue of ICECT 2014 - Held during September 01, 2014 in The Golkonda Hotel, Hyderabad, India

A New Approach for improving performance of Data Leakage Detection System

G.Rajesh Chandra, Dr.K.RamChand H Rao

Asst Professor, Dept. of ECM, K L University, Guntur, INDIA grajeshchandra@kluniversity.in
Professor, Dept. of CSE, **Dr.K.Ramchand H Rao[1]Dr**, INDIA, ramkolasani@gmail.com

Abstract *:* Now a day, in the real world the data of organizations will be appeared in other irrelevant websites. The scope for data leakage is very wide, and not limited to just email and web. We are all too familiar with stories of data loss from laptop theft, hacker break-ins, and backup tapes being lost or stolen, and so on. It is possible only by Data Leakers and those data leakers are trusted agents only. To identify the Data Leaker is very big task. By using Watermarking and fake data addition methods we identified leakers in olden days. But in those methods reliability and consistency is very low. In this paper we are providing high level security for data by using new approaches such as watermarking and fake data addition methods.

Key words : Watermarking, Guilty party, Forged Data

INTRODUCTION

This paper examines the data leakage and how it can impact an organization. In olden days for identifying the leaker is done by using fake data method in that method security is low. Third party can easily identify the fake data and easily removing it. So that it is failure model. We propose the new approach that provides the high level security. Every organization can handled trusted agents with responsive data by sharing it. After some time that responsive data may be available in untreated places those may be a unknown websites. The scope for data leakage is very wide, and not limited to just email and web.

WATER MARKING [1]

Watermarking technique is olden techniques. From hundreds years we are using these techniques but here we are providing a new algorithm for water marking concept this algorithm provides high securable water marking. In this paper first our task is to add watermarking image to the original data. Here we are developing a new watermarking technique that will takes input with an image and gives a unique watermarking image that may be useful for our approach this approach can be developing in the following algorithm

Input:

– f is the original image of sizeM1 ×M2,
– w1 is an set that is belongs to {− 1, 1} it is a digital watermark image with the range N1 × N2.

In this algorithm we are giving the input f, W1. The process of algorithm works as,

Algorithm[3]

1. Initiate l is from 1 to L

2. Initiate s from 1 to S generate s1(a,b)

3. Bring into being key Key1 ∈ {0, 1}
 if Key1 is zero then don't entrench a spot other wise
– sort the specified coefficients as:
fs1, l(a, b) _ fs2,l(a, b) _ fs3,la, b)

– do quantization by divide fs1,l(a, b) and fs3,l(a, b) into bins using the Following form Δ = (fs3,l(a, b) − fs1,l(a, b)) / (2Q – 1) .

4. The compound convert coefficients in each band are scaled back to the levels of the original image transform coefficients using the min and max coefficient Values.
◦ the fused coefficients fuseed are computed as follows:
Fused = αfs,l(a, b) +W(i, j).

5. An converse make over is now computed to give the watermarked image

Output:

Water marking image

The output of this algorithm gives image of watermarking. Next our task is to add this message with the data. The watermarking concept will be common to data of every trusted agent of organization.

Adding Forged Entities:

Forged Entities plays important role in our paper. Without these entities data administrator didn't distribute the data to the parties. Here forged entities are look like the original data. There is no difference between original data and forged data here we have to create forged data then adding it to original data and distribute it to parties. For creating forged data, we have so many algorithms. Here our task is to generate forged data depending on original data we are generating forged data. That data must and should be look like a original data and relative to the original data.

Generation of forged entities:

The generation of a forged entity for agent Ui as a black-box function CREATEFORGEDDATA(Ri, Fi, Condi), that automatically catches input as set of all data Ri, the subset of forged entities Fi that Ui has received so far and Condi and returns a new forged entity. This function wants Condi to gives a valid object that satisfies U's condition. Set Ri is needed as input so that the created forged entity is not only valid but also identical from other original entity.

GUILTY PARTY

The agent who concerned as a job of leaker the odds value as not official to receive data to the total number of agents data from owner or. Before we present the general formula for calculating the probability P{Gu|Sa} that an Process agent Ui is guilty, we provide a simple example. Assume that the distributor2 set O, the agent sets A and the target set S are:

O = {o1, o2, o3}; A1= {o1,o2}; A2= {o1, o3}; S = {o1, o2, o3};

In this case, total three of the owner's objects have been leaked and appear in S. Let us first consider how the target may have obtained object o1, which was given to both agents. The target either guessed o1 or one of A1 or A2 leaked it. We know that the probability of the former event is p, so assuming that probability that each of the two agents leaked o1 is the same, we have the following cases:

The target guessed d1 is leaked with probability p,

- Agent A1 leaked o1 to S with probability (1-p)/2
- Agent A2 leaked o1 to S with probability (1-p)/2.

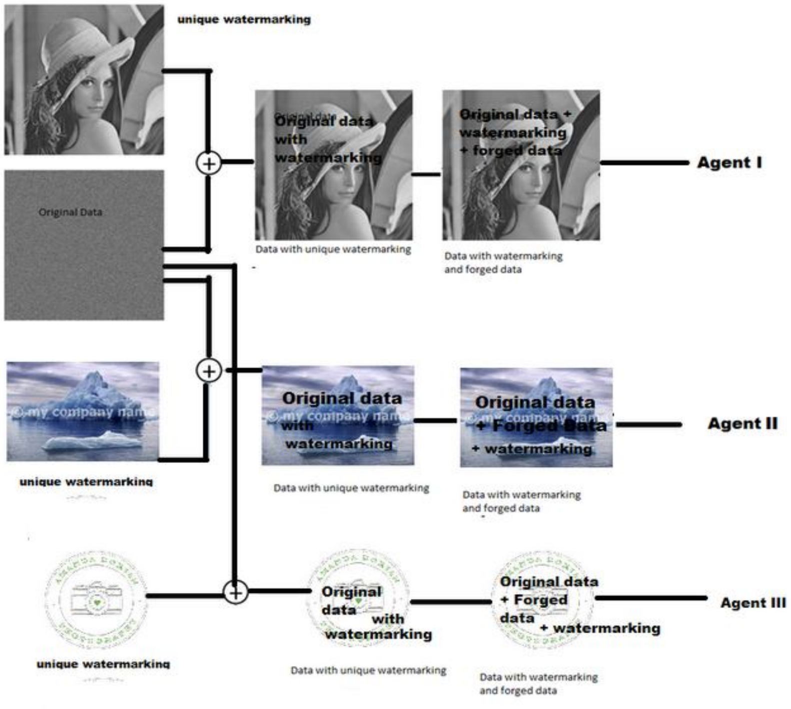
unique watermarking
Original Data
Original data with watermarking
Data with unique watermarking
Original data + watermarking + forged data
Data with watermarking and forged data
Agent I
© my company name
unique watermarking
Original data © my company name with watermarking
Data with unique watermarking
Original data © my company name + Forged Data + watermarking
Data with watermarking and forged data
Agent II
unique watermarking
Original data with watermarking
Data with unique watermarking
Original data + Forged data + watermarking
Data with watermarking and forged data
Agent III

Fig 1: Process of new approach

EXPLANATION OF PROCESS

Distributer always distributes the data to trusted agents. Those agents may be leaks the data .
So in our process we can generates a unique watermarking images and those images are adding to original data by distributer after that we can get a data with watermarking. Next we can generate the forged data by algorithm we can add the forged data to data with watermarking. Then we can get original data with forged data and watermarking. That data will be distributes to agents by data distributer

Let us take one example, for the explanation of this process, in any organization the owner always sharing its data to trusted worked workers after some days that data may be available in other websites or implementation of that data by any other organizations automatically that organization is damaged. Our paper gives a new approach for these types of problems in this approach the data administrator generates a new unique watermarking image and fake data these two are adding to original data. That will be distributes to agents if any agent works as a leaker then owner can identify him/her.

For this concept we have so many algorithm and techniques for identifying the leakers. But we are giving high level security to this concept.

CONCLUSION AND FUTURE WORK

In our paper we proposed a new concept on Data Leakage Detection system. In this system original data is added to watermarked image and after completion of this process that data will be added to forged data after that it will be distributed to agents if any where it will be founded we will identify the leaker easily for future work we may be encrypt that original distributed to agents. In this paper we given just a approach in our future we will develop a new project for data distributers with encryption algorithm for original data

REFERENCES

1.A Copyright Protection using Watermarking Algorithm INFORMATICA, 2006, Vol. 17, No. 2, 187–198 @ 2006 Institute of Mathematics and Informatics, Vilnius, Abou Ella HASSANIEN

2. International Journal of Computer Applications (0975 –8887) Volume 42–No.6, March 2012 25,Guilt Model Process for Identifying Data Leakage and Guilty Agent in Data transmission,.

3. Digital watermarking: A Tutorial, Dr. Vipula Singh Professor and Head of Electrical and Computer Engineering Department Geethanjali College of Engineering and Technology, Hyderabad India