Implementation of Digital Watermarking Technique to Secure IPR of Web Application Code

Himanshu Rastogi, Birendra Kumar Sharma

Abstract*: Theft of software code is rapidly increasing with the growth of internet all over the world. That becomes the serious issue for the creator of the software code, as they invest their time and money to develop software code. Code for the Web based application can be accessed easily, as they are available as open source. These software codes can be tempered and can be misused any time. The protection of such web application code is essential. For the security of such codes from unauthorized accessibility, number of protection methods have been designed and developed. A model was proposed by Himanshu et al [4] for the protection of copyright of software code. In which few extra character stings were embedded in the encrypted original string. In this model concept of cryptography was implemented. This research paper is presented as the implementation procedure of the Digital Watermarking Technique to secure Intellectual Property Right of the web application code developed in ASP.NET using Visual C# programming language.

Keywords* : Algorithm, Detection, Digital Watermarking, Encryption, Embedding, Intellectual Property Right, Web enabled application.

I. INTRODUCTION

A number of web enabled applications are running over the network as the Internet facility is increasing day by day, to provide the facilities to the end users. They are using these web enabled applications to improve the efficiency and effectiveness of their business work by reducing cost, provide fastest accessibility and secure transaction etc. The main drawback of the development of Web enabled Application uses is that the code is required to be put publically. This code may be accessed by any unauthorized user by entering into the system. Such unauthorized user can temper, and misuse this software code. Protection of such software code is necessary. The protection can be done by Intellectual Property Right using Digital watermarking. Intellectual Property (IP) is described as any "original creative work manifested in a tangible form that can be legally protected". Intellectual Property rights, means to control the method IP is used, accessed or distributed. The IP laws were enforced throughout the world by World Intellectual Property Organization (WIPO). With the help of protecting IP, we want to promote creativity and encourage the creator.

Manuscript published on 30 September 2019.
*Correspondence Author(s)

Himanshu Rastogi*, Research Scholar, Mewar University, Chittorgarh, Rajasthan, India. Email: himanshu_ras@yahoo.com
Dr. Birendra Kumar Sharma, Professor and Head, Department of MCA, AKG Engineering College, Ghaziabad, India. Email: bksharma888@yahoo.com

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

In year 2018, a global survey report was released by the Business Software Alliance [2]. Which shows the rate of illegal use of software in various countries is shown in Table 1.1.

Table 1.1: Unlicensed Software Installation Rates in percentage

Country Name	Years			
	2011	2013	2015	2017
Asia Pacific	60%	62%	61%	57%
C & E Europe	62%	61%	58%	57%
Latin America	61%	59%	55%	52%
ME & Africa	58%	59%	57%	56%
N America	19%	19%	17%	16%
W Europe	32%	29%	28%	26%

It means privacy of software directly affects the revenue of software vendors. The software vendors are loosing millions of US dollars every year. Last four (alternative) year data have been shown in Table 1.2

Table 1.2: Amount of Loss in $

Country Name	Years			
	2011	2013	2015	2017
Asia Pacific	$20,998	$21,041	$19,064	$16,439
C & E Europe	$6,133	$5,318	$3,136	$2,910
Latin America	$7,459	$8,422	$5,787	$4,957
ME & Africa	$4,159	$4,309	$3,696	$3,077
N America	$10,958	$10,853	$10,016	$9,458
W Europe	$13,749	$12,766	$10,543	$9,461

Digital Watermark technique was actively came into existence in the mid of 1990s, for copyright protection, and intellectual property right etc for digital contents or documents that are either in any form like image, video, or text. In digital watermarking a pattern is embedded in the original IP such that actual working cannot be disturbed. Different methods have been discussed time to time to protect software code from piracy and unauthorized accessibility and tempering. In software watermarking technology, a security or special key will be embedded into the original software code, to prove the ownership in such a manner that it would not disturb the actual code[5][10]. This embedding can be done either at design time or at run time.

This security or special key or watermark can be extracted when required to prove ownership. Security and piracy of software become an important issue. The secret key includes data of the actual owner like developer and IT Company, developed that code. The flow of the application program cannot be disturbed by an embedded watermarked. This will not affect the application code. [11]. Software watermarking can be enhanced with other forms of protection, copyright infringement and decompilation [12].

It has been observed that web based application plays a major role in any transaction over Internet [1]. All the sectors are taking the advantage by using these Web applications. And so any one as individual or a company wants to create an web application without putting much efforts towards the development of such web applications. Such developer wants to get code form the internet and they implement the same code in their websites. Hence, protection of software code putting publically and in the visible form is major issue.

Protection model for web enabled application code is developed by using ASP.NET and C#. Microsoft developed ASP.NET which is an open-source web application framework designed for the development of dynamic web sites, and services. The main advantage of using ASP.NET is to reduce the programming code which is required to implement protection model. It was first released in January 2002 under .NET framework. This framework allows web developers to write code with the help of any .NET language like visual C# [14].

Watermarked module is implemented in the form of DLL file, to prevent it from unauthorized access. A DLL is a library contains functions and data which can be used by more than one program at the same time. These dll files are registered with GAC (Global Assembly Cache) to make it shared assembly. So that it can be accessed from its original location. To make it shared assembly a strong name key must be required [15][16].

II. RELATED WORK

Ashwag Alrehily et al [3] proposed a Return-Oriented Programming (ROP) based software watermark design. In their research paper they considered that to improve the efficiency of the software watermarking security, a secured Hash algorithm plays an important role. In the method discussed, they focused on categories and analysis of the gadgets. H. Rastogi et al [4] proposed a method of embedding an encrypted key in the original data. In this research paper, the technique of cryptography was implemented with an assigned key and also explained the working procedure of the technique. Nisha [6] has done survey based on various techniques of watermarking and, further, explained the comparison between different techniques on the basis of experimental results. Advantages and disadvantages of these techniques of watermarking were also discussed in her research paper.

Atef Zaki Ghalwash et al [7] proposed a technique, which embeds and detects the watermark in the data structure of software. The technique works on two different stages in which Variable-base Factorial generated watermark is embedded in a Quad-tree data structure. In the second stage, the extracted watermark is compared with the actual data to find out the accuracy and reliability of detecting the watermark.

Vasudev [8] suggested that the vast popularity of internet presents different multimedia resources through different digital networks. These multimedia resources or digital media must be secured against various unauthorized attacks.

Kaur et al [9] proposed a innovative method for the protection of digital contents using digital image watermarking. In this proposed method author, presented a technique using a combination of spatial domain technique and frequency domain techniques.

Dwivedi et al [11] proposed a database watermarking techniques with constraints and analyze the strengths and weaknesses. They suggested in their paper that in todays digital scenario not only images related contents, video enabled data, and audio based data are in digital form, but relational databases also have been migrated towards in digital form. These databases are used as a service in the applications in different forms like finance related databases, multimedia related databases, personnel related databases etc. It is not so easy to embed Digital Watermarking in relational database without losing the integrity because databases have very little redundancy, if we compared with multimedia data.

For the protection of digital contents, Awasthi et al [12] proposed a technique for Digital Image Watermarking. Technique presented in the proposed model is based on the mixture of Spatial Domain Technique (SDT) and Frequency Domain Techniques (FDT. Three different techniques used in watermarking viz Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD) and Least Significant Bit Techniques (LSBT) are combined to give strength to the watermarked image and also to get better the quality of watermarked image.

Sharma et al [13] explained static and dynamic techniques for software watermarking. In their research paper, they discussed that the watermarks are embedded in the source code at the time of coding of the application, in static software watermarking techniques. While in dynamic software watermarking techniques the watermarks are generated at run time or during execution time and embedded later at run time. In their paper, they have discussed about the Modular Programming and also proposed a new static watermarking technique for the same

III. DIGITAL WATERMARKING TECHNIQUE

a) **For Embedding:** Following is the proposed algorithm for embedding code was described by H.Rastogi et al [4]. In this algorithm, actual text string will be first encrypted by using some algorithm. This encrypted text will then combine with a watermarked key. Combination of these two values will then processed by embedding function to form a watermarked text character string. This Watermarked code can be displayed on the website at any place. The representation of algorithm is shown in the figure (1). Mathematical representation of the algorithm is as follows:

$$\sum_{i=1}^{n} C_E = f\left(\sum_{i=1}^{n} C_O\right) \qquad \text{………. (1)}$$

$$\sum_{i=1}^{32} C_W = \sum_{i=1}^{n} C_E + \sum_{i=n+1}^{30} C_R + \sum_{i=31}^{32} C_L \qquad \text{………. (2)}$$

Where $C_O \Rightarrow$ Original Character String

$C_E \Rightarrow$ Encrypted form of C_O

$C_w \Rightarrow$ Watermarked Character String

$C_R \Rightarrow$ Random Character String

$C_L \Rightarrow$ Character String based on the character length of C_O

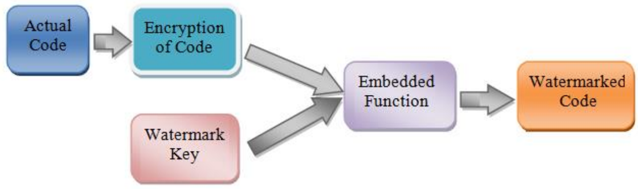

Fig: 1. Embedded Code Algorithm Method

Watermarking Algorithms: Following are the two algorithms used in this paper. Abbreviations used in the algorithms are shown in table 3.1:

Table 3.1 : Abbreviations used in Algorithm

Sr.No	Abb Used	Purpose
1.	**AV**	Actual Value
2.	**ENV**	Encoded Value
3.	**RS**	Random Character String
4.	**CL**	String CL to find out length of Actual Value
5.	**nOP**	Number at Once Position
6.	**nTP**	Number at Tense Position
7.	**nAV**	Length of Actual Value
8.	**EXV**	Extracted Value
9.	**OV**	Observed Value

3.1 Embedded Code Algorithm:

```
Read: (AV);
n = Length(AV)
for i =0 to n-1 do
        ENV_i = Char(Int(AV_i) + 3)
end for;
 Generate string of random characters RS_{30-n};
for i=0 to 30-n
      RS_i = RS_i  + Char(RandomNo);
end for
ENV = append(AV, RS);
Define string CL with 10 different characters
nOP  =  n  / 10;
nTP  = n Mod 10;
ENV = append(ENV, CL(nTP) , CL(nOP));
```

b) **For Extraction:** This algorithm is the reversible process of the algorithm used in Embedded code. In this algorithm, Watermarked code will be split on the basis of the last two character code of the embedded code. These two character code will be converted in to number system form to get the length of actual text string. Let say it is ‘n’. After that, first ‘n’ characters of the watermarked code will be split and decrypt with the same key as used in the embedded code algorithm.

If it is found as same as embedded during watermarked code, then the code owner is authenticated otherwise the user is fake.

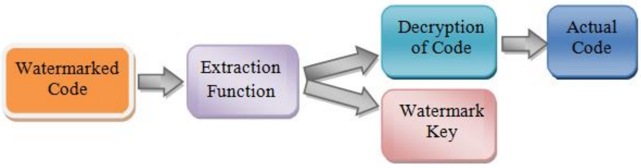

Fig: 2. Extraction of watermark code algorithm Method

3.2 Extraction of Watermark Code Algorithm:

```
Input(ENV);
Extract last two characters from ENV and find the
      index of these characters from string CL, defined in
      algorithm (2).
Find the Length of string (CL) and assign it to nCL;
for i =0 to nCL
    if last value of ENV matched with CL_i then
        nOP = i;
    end
    if second last value of ENV matched with CL_i then
        nTP = i;
    end
end for
Find length of AV by nAV= 10 * nTP + nOP;
Extract first nAV characters from ENV
for i = 0 to nAV -1
      EXV_i = EXV_i + ENV_i;
end for
for i =0 to nAV-1 do
        OV_i = Char(Int(EXV_i) + 3)
end for;
if OV is same as AV then
      ownership PASS
else
      ownership FAIL
end
```

IV. IMPLEMENTATION OF TECHNIQUE IN WEB APPLICATION DEVELOPED IN ASP.NET

Above algorithm has been implemented in web enabled application using ASP.NET framework and Visual C#. For the execution of the algorithm, functions for Embedding and Extraction are defined in .dll file. To create .dll file, we have to select .

Retrieval Number: K21720981119/19©BEIESP
DOI: 10.35940/ijitee.K2172.0981119
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

NET Framework (Class Library) during selection of a new project in visual studio. Here we wrote these functions and compiled this code using Build Solution option, to create .dll file.

This created .dll file need to be registered as shared assembly so that it can be used by more than on user at the same time. For registration, we need to use visual studio command prompt and write the following command to create strong name file:

C:\sn –k "*Path of the location where snk file will be saved"*

With this command we have created strong name file. Added this file into ASP.NET file, where we have used these functions. To add reference of this strong name file following sequence of the procedure was followed:

Project Menu → Properties→ Signing→ "Here check option *Sign the Assembly*"

And select the .snk file (Strong Name File), using browse option.

Again rebuild the code to update .dll file.

Now, this .dll will need to register with GAC (Global Assembly Cache) by using visual studio command prompt with the following syntax:

C:\ gacutil –I "*Path of the .dll file*"

This will attach with GAC.

Now this .dll is ready to connect with any .aspx file or project.

Function definition used in .dll file:

```
namespace WebApplication
{
   public partial class clsValidationCheck
   {
      protected string EncryptString(String strText)
      {
         //-------------Code For Encryption of String
         //-------------code for random char generation---------
         //-------------code to add two additional numbers for
                                                        length
      }

      protected string DecryptString(String encString)
      {
         //-----code for extraction of original string length &
                                            encrypted string
         //-----code for conversion in to original string--
      }
   }
}
```

Function call in .aspx file:

```
namespace WebApplication
{
   public partial class myWebPage : System.Web.UI.Page
   {
      protected void btnEncrypt_Click(object sender,
                                             EventArgs e)
      {
          clsValidationCheck objClass = new
                                     clsValidationCheck();
         objClass. EncryptString(strString);
      }
      protected void btnDecrypt_Click(object sender,
                                             EventArgs e)
      {
         clsValidationCheck objClass = new
                                     clsValidationCheck();
         objClass.DecryptString(strString);
      }
   }
}
```

V. PERFORMANCE EVALUATION METRIC FOR WATERMARKED WEB APPLICATION

The performance of any software code is always based on space consumed by the system, speed of the processor and time taken for the execution of the application. For the evaluation of the performance of watermarked web enabled application code, mathematically it can be expressed as follows:

The size of the watermarked web enabled application code should not increase significantly as a web server hosts lots of web applications. Let the size of an actual web application code (Actual Value) 'x' be $S(x)$ and also let the size of the web application code after watermarking (Watermarked Value) 'W(x)' be $S(W(x))$, the performance (W(x),x) of web enabled application code is expressed as:

Performance of watermarked Code (W(x), x)

= ((Actual Value – Watermarked Value)) / Actual Value

$$= [S(x) - S(W(x))] / S(x)$$

VI. CONCLUSION

As we know that Web enabled application plays a major role on internet for every sectors of any business like Education, Healthcare, Automobiles, etc. For the analysis of the protection of software code for web application, different research papers were surveyed. In our research paper, in which an expected model was developed for the protection of copyright of software code using digital watermarking, we have implemented the same model using ASP.NET framework and Visual C#. In this research paper, we have discussed about the algorithm with mathematical representation and also the steps involved in using the model. This implementation could be either in visible form or in invisible form.

REFERENCES

1. Himanshu Rastogi, Dr. B.K.Sharma "Web Based Application Protection using Software Watermarking: A Study" in the *2nd International Conference on Managerial Strategies for Technological Transformations in 21st Century, 2019*, ISBN: 978-93-86789-82-2, Chapter ID: IC-MSFTTI21C/YB/AP-18, pp.135-139.
2. Software Management: Security Imperative, Business Opportunity, BSA Global Software Survey, June 2018
3. 2018 Computer Security and Software Watermarking
4. H. Rastogi, B.K. Sharma, "Development of an expected model for the protection of Copyright of software code using digital watermarking", *International Journal of Computer Sciences and Engineering*, Vol.6, Issue.5, pp.378-382, 2018.

5. S. E. Tsai, K. C. Liu, and S. M. Yang, “An Efficient Image Watermarking Method Based on Fast Discrete Cosine Transform Algorithm”, *Hindwani-Mathematical Problems in Engineering*, Volume 2017, Article ID 3509258.
6. Nisha, “Digital Watermarking Techniques: Review”, *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 7, Issue 1, (2017), ISSN: 2277 128X.
7. 2017 A Watermark Methodology for Software Copyright Protection
8. Rajiv Vasudev,“A Review on Digital Image Watermarking and Its Techniques”, *Journal of Image and Graphics*, Vol. 4, No. 2, (2016), page no 150-153
9. Maninder Kaur and Nirvair Neeru. “Digital Image Watermarking using New Combined Technique”, *International Journal of Computer Applications*, (2016), 145(2):26-30.
10. Sumedh P. Ingale et al, “Digital Watermarking Algorithm using DWT Technique”, *International Journal of Computer Science and Mobile Computing*, Vol.5 Issue.5, (2016), pg. 01-09
11. Anuj Kumar Dwivedi, Dr. B. K. Sharma, Dr. A. K. Vyas, “Watermarking Techniques for Ownership Protection of Relational Databases”, *International Journal of Emerging Technology and Advanced Engineering*; ISSN 2250-2459 (Online), Volume 4, Special Issue 1, (2014) *International Conference on Advanced Developments in Engineering and Technology* (ICADET-14), INDIA.
12. Yogesh Awasthi, R.P.Agarwal, B.K. Sharma, “Intellectual Property Right Protection of Browser based Software through Watermarking Technique”, *International Journal of Computer Application(IJCA)*, Volume 97– No.12, (2014), 32-36
13. Dr. B. K. Sharma, Dr. R. P. Agarwal, Dr. Raghuraj Singh, “An IPR of software codes using watermarking For Modular Programming”, *ISST Journal of Mathematics & Computing System*, ISSN No. 0976-9048, Vol. 1 No.1, (2010), p.p. 55-58
14. https://en.wikipedia.org/wiki/ASP.NET
15. https://support.microsoft.com/en-in/help/815065/what-is-a-dll
16. https://www.c-sharpcorner.com/article/assembly-in-net/

AUTHORS PROFILE

Himanshu Rastogi has completed his MCA from CCS University, Meerut in 2000 and M.Phil. in Computer Science from Alagappa University, Tamilnadu in 2004. He is currently pursuing Ph.D. from Mewar Univerisity. His academic experience is approx 16 Years. His research interests include Digital Watermarking, Data warehousing, Data Mining and, Computer Networking. He has published his research papers in International/National Journals/Conferences. He has the experience of all phases of SDLC and PDLC to deliver business focused solutions as Technical/Team Lead, Developer.

.

Dr. Birendra Kumar Sharma is a Professor and Dean Hostel of Ajay Kumar Garg Engineering College, Ghaziabad. He has obtained his MCA degree from JNU, New Delhi, M.Tech. from Guru Gobind Singh Indraprastha University, Delhi and Ph.D. from Shobhit University, Meerut. His areas of specializations are Watermarking, Digital Watermarking, Software Watermarking & IPR. During his career of 18 years experience in the teaching, he has published many books for UG & PG students of engineering like Discrete Mathematics, Theory of Computation, Computer concepts and programming in C etc and many research papers in International/National Journals/Conferences.

Retrieval Number: K21720981119/19©BEIESP
DOI: 10.35940/ijitee.K2172.0981119
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.