# Development of an expected model for the protection of Copyright of software code using digital watermarking

**H. Rastogi[1*], B.K. Sharma [2]**

[1*]Research Scholar, Mewar University, Chittorgarh, Rajasthan, India
[2]Department of MCA, AKG Engineering College, Ghaziabad, India

[*]*Corresponding Author: himanshu_ras@yahoo.com, Tel.: +91-97170-53216*

*Abstract:* The research done in this paper aimed to develop a model for the protection of copyright of software using Digital Watermarking by providing a proper way for designing the software. Digital watermarking has now become the research area for the protection of intellectual property right. In this research paper, the technique of cryptography with a assigned key is implemented for the development of the model. This paper gives the procedure of the implementation of the technique.

*Keywords*— Copyright, Digital Watermarking, Algorithm, Encryption, Embedding, Detection.

## I. INTRODUCTION

In today's era the most valuable assets of IT industry is business applications or application software, as Internet and communications technology is growing. It means that in the next era everything related to the business will be done through these business applications. With the growth of such softwares, this will increase threats like piracy. For the protection of software code, protection of copyright is also required. Digital watermarking is the good method by which one can prove the ownership.

With the fast growth of IT, the significance of digitization has become greater than before. Now a day, most of the people is sharing their original contents using the internet facility. That means it is,now, necessary to protect such original/licensed content, for unauthorized use and also not able to make forged copies of such original contents [3].

| Country Name | Years | | | |
|---|---|---|---|---|
| | **2009** | **2011** | **2013** | **2015** |
| **Asia Pacific** | 59% | 60% | 62% | 61% |
| **C & E Europe** | 64% | 62% | 61% | 58% |
| **Latin America** | 63% | 61% | 59% | 55% |
| **ME & Africa** | 59% | 58% | 59% | 57% |
| **N America** | 21% | 19% | 19% | 17% |
| **W Europe** | 34% | 32% | 29% | 28% |

**Table 1.1: Unlicensed Software Installation Rates in percentage**

Further, as per the global survey released by the Business Software Alliance [6] the rate of illegal use of software in various countries like Asia Pacific, Central and Eastern Europe( C & E Europe), Latin America, Middle East and Africa(ME & Africa), North America ( N America) and Western Europe(W Europe) is shown in Table 1.1.

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

| Country Name | Years | | | |
|---|---|---|---|---|
| | **2009** | **2011** | **2013** | **2015** |
| **Asia Pacific** | $16,544 | $20,998 | $21,041 | $19,064 |
| **C & E Europe** | $4,673 | $6,133 | $5,318 | $3,136 |
| **Latin America** | $6,210 | $7,459 | $8,422 | $5,787 |
| **ME & Africa** | $2,887 | $4,159 | $4,309 | $3,696 |
| **N America** | $9,379 | $10,958 | $10,853 | $10,016 |
| **W Europe** | $11,750 | $13,749 | $12,766 | $10,543 |

**Table 1.2 : Amount of Loss in $**

It is very common to copy a part of the software or full software to be copied through internet without any knowledge of the software programmer or company or owner.IT companies are spending lots of money and efforts to provide the best business solutions to the business industries. These efforts should be protected. Cyber Laws have great importance for the protection of copyright.

Application software for business solutions is the main part of the software company; therefore, it is necessary to protect the copyright of such software. For this, it is required to have an effective method or model for the protection of copyright, so that any kind of modification in the code can be identified.

Digital watermarking is a significant technology having many applications. A number of watermarking schemes have been discussed for images, audio, and video streams. In digital watermarking a key pattern will be embedded at the initial level and later on, when required, it is detected to identify the ownership. Digital watermarking is the embedding or hiding of information within a digital file without noticeably altering the file itself. Now digital image watermarking is increasing attention due to the fast developing in the internet traffic. Digital watermarking achieved is popularity due to its significance in content authentication and copyright protection for digital multimedia data. It is inserted invisible in host image so that it can be extracted at later times for the evidence of rightful ownership [9].

This paper focuses on the watermarking in the software code. In this paper, an algorithm is proposed as a model. Section II presents the related work done for the protection of copyright for software code. Section III elaborates on the application and technique of digital watermarking, which explains the embedding and detection algorithms with the help of an example. Finally, the conclusions are presented in Section IV.

## II.  RELATED WORK

Neha [1] has done survey of various techniques of watermarking and, explained the comparison between different techniques based on experimental results. In this paper, she has also discussed about advantages and disadvantages of these techniques of watermarking.

Tsai et al [2] proposed watermarking method for an image based on the fast discrete cosine transform (DCT) algorithm for implementation in digital signal processor. In this paper they proposed keys in watermarking process, which include four frequency coefficients in DCT, two random permutation vectors, and a quantization matrix for normalizing the watermark and the host image. They used fast DCT algorithm to reduce the complexity of two-dimensional image transformation, so that embedding/decoding image watermark can be completed in real time within a time frame.

M. Jamal et al [4] was proposed a non-blind Digital Image Watermarking method which  is the fusion of "Redundant Discrete Wavelet Transform (RDWT) and Singular Value Decomposition (SVD)" in YCbCr color space. This scheme has been tested against different geometrical transformations.

S. Mudassar et al [5] has used hybrid DWT-SVD based colour image watermarking by which unauthorized person cannot get the hidden information. In this paper, author used the DWT-SVD method to divide the colour into R, G and B sub-channels.

Vasudev[6] suggested that the enormous popularity of internet offers various multimedia resources through various digital networks. These multimedia resources or digital media should be protected against various unauthorized attacks so as to use them for profit or security. Digital Watermarking is a way of protecting the digital media from unauthorized usage. This paper is a review on the Watermarking process, Types of watermarks, Various Watermarking Techniques and Applications of Watermarking.

Kaur et al [7] proposed a new method of digital image watermarking for the protection of digital contents. In this proposed method author, presented a technique using a combination of spatial domain technique and frequency domain techniques. Discrete wavelet transform, singular value decomposition and least significant bit techniques are combined to provide robustness to the watermark image as well as to improve the quality of obtained watermarked image.

Ingale et al [10] approached, in his research paper, for watermarking image and extracting it for authentication purposes. As digital watermarking has turn into a promising research area to face the challenges due to the growth in sharing of digital content on the internet. Digital watermarking techniques are very useful, to avoid misuse of this data. In this technique, a message (visible or invisible) called as a watermark is embedded into data which again could be used for various applications like copyright protection, authentication etc.

Dwivedi et al [11] proposed a database watermarking techniques with certain constraints and analyze the strengths and weaknesses. They suggested in their paper that in current digital scenario not only images, video, and audio are in digital form, but relational databases are also digitized and used as a service in the applications, including finance databases, multimedia databases, personnel databases etc. various digital watermarking techniques have been proposed for dealing with security, authentication ownership protection and piracy control of digital contents.

Awasthi et al [12] proposed a method of digital image watermarking for the protection of digital contents. This proposed method presents a technique which is based on combination of spatial domain technique and frequency domain techniques. Discrete wavelet transform, singular value decomposition and least significant bit techniques are combined to provide robustness to the watermark image as well as to improve the quality of obtained watermarked image.

V.Kapoor[13] proposed an integrated cryptographic scheme, message digest algorithm MD5 and RSA Algorithm and an Encryption Algorithm to verify the integrity of the message.

Sharma et al [14], proposed a method, A variety of prevention techniques have been developed for copyright protection of software codes or intellectual property rights (IPR) using both hardware and software. But, unfortunately no single technique is currently strong enough to protect the software codes. However, through a combination of techniques software developer can better protect their software codes. In this paper, they have explained mainly static and dynamic techniques of software watermarking.

## III. APPLICATIONS AND PROPERTIES

Digital Watermarking is a technique for the protection of copyrights and authenticating the original contents. Using this technique, we need to embed a visible or invisible mark or string in the software code on the basis of some logic. Later on, when required, this watermarked string may be checked for the authentication of the original content. For that we have proposed two algorithms one for embedding and another for detection.
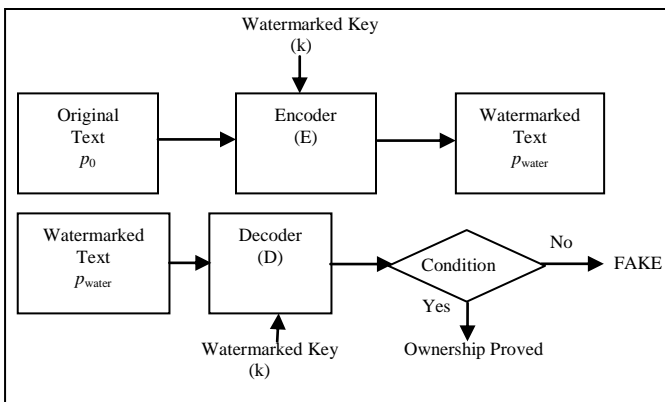


**Fig: 1. Embedding and Detection of digital watermark**

$p_0$         = OriginalInput
$p_{water}$     = Watermark($p_0$,key)
where key = codedValueof($p_0$) + RandValues(30-len($p_0$)) +
          sizeof($p_0$)

### Algorithm for Embedding:

a. Declare an array, which consists of 'a' to 'j' characters from 0 to 9 index values.

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|
| a | b | c | d | e | f | g | h | i | j |

b. Read input IS (Input String).
c. Find the length of IS.
d. Encrypt IS in to ES(Encrypted String) by replacing each character by 5 characters ahead.

e. Insert 30 – length(ES) characters in random order.
f. Insert last two characters from the array defined in step a, on the basis of the length of the ES. For example of the length is 6 characters then considering it as 06 and the corresponding character set is {0-'a',6- 'g'}.
g. Now this Encrypted String consists of First 'n' characters of encrypted IS, plus random character sets, and last two characters for the length of original IS, in encrypted form.

### Algorithm for Detection:

a. Read ES (Encrypted String).
b. Read Last two characters. Find the index corresponding to the characters. Find 'n' using concatenation of index values.
c. Read first 'n' characters from ES.
d. Convert these in to original string (ISd), by replacing them 5 characters less.
e. Check for watermark:
f. if (ISd= =IS)
   {     // Ownership proved         }
   else
   {     // Fake User         }

### Algorithm Illustration with the help of an Example

### A. For Embedding:

a. Create an array of size 10.

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|
| a | b | c | d | e | f | g | h | i | j |

b. Let IS (Input String) is "Research".
c. Length of IS is 8 characters.
d. Encrypt String (ES) = {'W', 'j', 'x', 'j', 'f', 'w', 'h', 'm'}
e. Now generate 30-8=22 characters randomly and insert these characters in to ES.

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|----|
| W | j | x | j | f | w | h | m | g | h | 2 |

| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
|----|----|----|----|----|----|----|----|----|----|
| 4 | g | 6 | $ | ^ | @ | A | W | C | 4 |

| 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
|----|----|----|----|----|----|----|----|----|----|----|
| 2 | % | H | @ | * | ( | ! | C | T | | |

f. Now, read length 8(=08). Find the corresponding values from array {'a', 'i'}.
g. Insert these characters into ES.

      

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| W | j | x | j | f | w | h | m | g | h | 2 |

| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
|---|---|---|---|---|---|---|---|---|---|
| 4 | g | 6 | $ | ^ | @ | A | W | C | 4 |

| 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|
| 2 | % | H | @ | * | ( | ! | C | T | **a** | **i** |

This is now the watermarked string.

### B.  For Detection:

a.  Read Last two characters of ES={'a', 'i'}.
b.  Corresponding indexes are {0,8}. Therefore length is 08.
c.  Now extract first 8 characters from the ES. Which are:
d.

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| W | j | x | j | f | w | h | m |

e.  Replace these characters by 5 characters previous of these.

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| R | e | s | e | a | r | c | h |

f.  Now, check for watermarking:
   if ($IS_d = =IS_o$)          //$IS_d$ = Decoded IS and
   $IS_o$=Original IS   →*If ("Research"= "Research")*
   {   // Ownership proved   }
   else
   {   // Fake User   }

## IV.  CONCLUSION

In this research paper we surveyed a number of different kinds of watermarking techniques for software code, relational databases; images. The proposed algorithm will work in an efficient manner to identify authenticated ownership in the development of software code. This algorithm paid major focus on protection of copyright using digital watermarking. Usability of the watermarked software code leaves so many queries for future research.

### REFERENCES

[1] 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.

[2] Nisha, "*Digital Watermarking Techniques: Review*", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 7, Issue 1, 2017.

[3] Himanshu Rastogi, Dr. B.K.Sharma "*A Study on Intellectual Property Right and Digital Watermarking*", International Journal of Advanced Research in Computer Science, Volume 8, No. 7, Page No 368-371, 2017.

[4] M. Jamal, S. Mudassar, F. S. Mehmood, M. R. Rehman, "*Improved Consistency of Digital Image Watermarking Using RDWT and SVD*", International Journal of Scientific Research in Computer Science and Engineering, Vol.5, Issue.3, pp.104-106, 2017

[5] S. Mudassar, M. Jamal, F. S. Mehmood, M. R. Rehman, "*Resistance of Watermarked Image against Solidity Attacks*", International Journal of Scientific Research in Computer Science and Engineering, Vol.5, Issue.4, pp.31-35, 2017

[6] Rajiv Vasudev,"*A Review on Digital Image Watermarking and Its Techniques*", Journal of Image and Graphics, Vol. 4, No. 2, page no 150-153, 2016.[4]

[7] Maninder Kaur and Nirvair Neeru. "*Digital Image Watermarking using New Combined Technique*", International Journal of Computer Applications, 145(2), page no 26-30, 2016.[5]

[8] Seizing Opportunity Through License Compliance: BSA Global Software Survey, MAY 2016[6]

[9] J. K. Ravan, T.C.Thanuja "*Watermarking Technique for security*", International Conference on Recent Innovations in Engineering and Management, page no 721-725, 2016.[7]

[10] Sumedh P. Ingale et al, "*Digital Watermarking Algorithm using DWT Technique*", International Journal of Computer Science and Mobile Computing, Vol.5 Issue.5, page no 01-09, 2016[8]

[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. [9]

[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, page no 32-36, 2014. [10]

[13] V. Kapoor, "*A New Cryptography Algorithm with an Integrated Scheme to Improve Data Security*", International Journal of Scientific Research in Network Security and Communication, Vol.1, Issue.2, pp.39-46, 2013.

[14] 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, Vol. 1 No.1, page no 55-58, 2010.[11]

## Authors Profile

*Mr.* H. 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. and currently working as Associate Professor in the Department of Information Technology, IAMR, Ghaziabad since 2009. He is also certified from the Department of Electronics and ICT Academics, IIT Kanpur for 'R-Programming', 'Mobile Computing-A Practical Approach', and 'Python- A Practical Approach'. He also has the core knowledge of Advanced MS Excel. His academic experience is approx 16 Years. His research interests include Digital Watermarking, Data warehousing, Data Mining and Cloud Computing. 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.* B. K. 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.