INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 2)
Available online at: www.ijariit.com

Application of digital watermarking in piracy

Shrutika Potdar
potdarshrutika6@gmail.com
Infosys Technologies Limited, Mumbai, Maharashtra

Mihir Potdar
potdarmihir10@gmail.com
Rajiv Gandhi Institute of Technology, Andheri (West), Mumbai

ABSTRACT

In today's world where piracy has surfaced itself as one of the biggest problems it becomes important to protect the originality to prevent huge revenue losses, to safeguard digital rights and protect information. This paper presents the application of digital watermarking for authorization against copying or piracy. E-Banking is the method of banking in which the customer conducts transactions electronically via the internet which causes the problem of phishing. The remedy to avoid phishing is to use different anti-piracy techniques. The technique that we are using is digital watermarking. The watermark is inserted by means of a security key. On reception, only the authorized person with a valid security key can extract the watermark thus verifying the integrity and authenticity of the image.

Keywords: *Digital watermarking, Phishing, E-Banking, Algorithm, Three-Factor authentication.*

1. INTRODUCTION

Need for Anti-piracy appeared when people tried to pirate the software by different ways to avoid the actual payment for licenses. After putting endless efforts with intelligence if related operations online. When you will register for Online banking you will get login Id which is generated by the system and is Unique across all the registered users of that bank. In present image security digital watermarking is the widely used technique for protecting copyright for images, audio and video files. Because of these reasons, we are using Digital watermarking in E-banking to avoid phishing which will enhance the security and lead to Anti-Piracy.

2. FACTS AND FIGURES

Fig- 1 Most Targeted Industry Sectors 4th Quarter 2013

According to the report by Anti Phishing Working Group (APWG), Payment Services continued to be the most-targeted industry sector throughout 2013, representing nearly 54 percent of attacks.[3]

3. ALGORITHM

The two main parts of the process are:

- Hardware product key-Pen-drive
- Digital Watermarking process

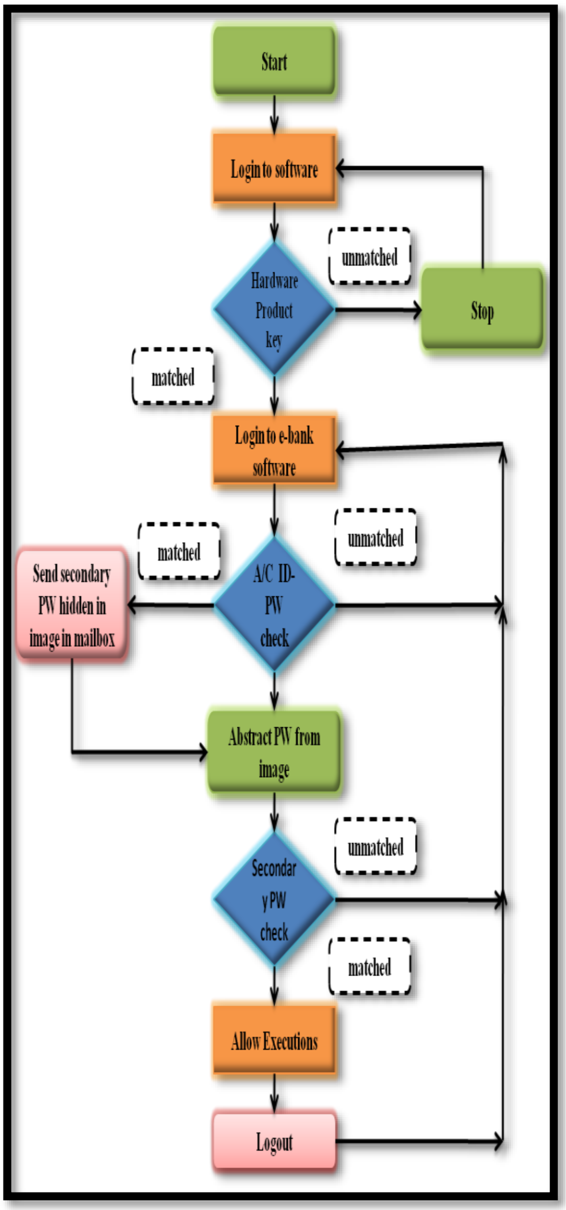

Fig-2 Algorithm for stimulation

4. TECHNICAL DETAILS

1) Hardware product key- Pen-drive

Pen-drive contains the source code and it is required to keep the software running.

2) Digital Watermarking Process

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal.

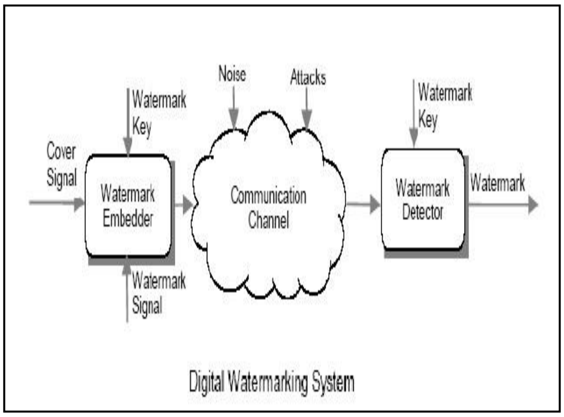

Fig-3 Digital Watermarking System

The wavelet decomposition decomposes the input image into high and low pass components with different orientations. For watermarking, a discrete wavelet transform (DWT) is applied to the original image.[1]

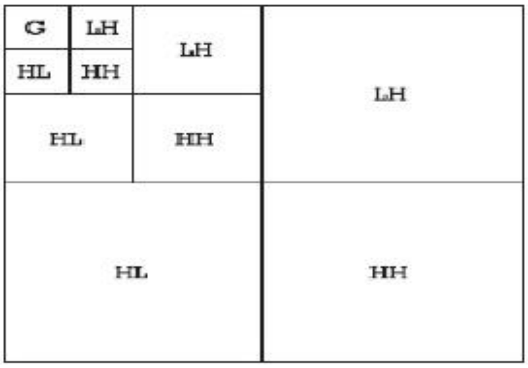

Fig-4 Tree level DWT calculation of the image

5. ADVANTAGES

- The hardware key is not in textual format but a pen drive is used and hence till your operating System detects the pen drive, owner application can run.
- Secured second layer authentication system by way of getting the password from the image that has been sent to the user on his registered email id on successful authentication.
- Second layer security login by way of content placed in the image attached to the Email sent to the user on the first login
- You can get real-time banking without calling or visiting bank branches.
- You will get real-time banking operations.
- Creation of a saving account, Current account.
- Creation of fixed deposit.
- Checking transactions performed in each account.

6. DISADVANTAGES

- Website performance – sometimes the website is too slow or not enough user-friendly.
- Little long learning curve especially for people who don’t know much about computer and internet.

7. APPLICATIONS

- **Authenticate content and objects:-**Verify that content is genuine, from an authorized source, and confirm that it has not been altered or falsified.

- **Complement existing security strategies:-**Add another layer of security to encrypted content in order to protect your assets and help identify the source of leaks.

- **Monitor broadcasts and internet distribution:-**Confirm specified content airs in a given market, at a specific time, and in its entirety. License compliance, advertising clearance verification, and detection of unauthorized use are also possible.

- **Manage digital rights:-**Connect content outside Digital Rights Management (DRM) systems back to usage rules, billing information, and other critical metadata.

- **Deter counterfeiting and piracy:-**Attach ownership information, usage rights, and copy/play control instructions to owned content.

Though there are several other techniques available for copyright protection and several other similar issues, digital watermarking is the only preferred algorithm because of its basic advantages like being robust, fragile and imperceptible. The proposed system signifies the use of a simple pen-drive which stops the unethical practice of piracy. It emphasizes the concept of digital watermarking and its contribution for developing multimedia data copyright protection. It explains how phishing has being curbed out due to which online banking has flourished.

8. FUTURE SCOPE

Three Factor Authentication

However, for a better security, a three factor authentication process should be considered. The third authentication factor is the use of biometric such as iris or thumbprint recognition. This ascertains who one is, biologically. This method of authentication has been introduced by the Employee Provident Fund (EPF) for it members but is limited to getting the latest statements of a member. With a three-factor authentication, a more secure method can be implemented - a password to ascertain what one knows, a token (smartcard) to ascertain what one has, and biometric recognition (for example fingerprint or thumbprint) to ascertain who one biologically is. As such, if passwords have been compromised, fraudsters need to get through another two levels of authentication to access a customer's account. This would be difficult, if not totally impossible.

9. REFERENCES

[1] (http://www.digimarc.com/technology/about-digital-watermarking)
[2] (http://www.digitalwatermarkingalliance.org/app_auth.asp)
[3] (http://www.apwg.org/report-phishing/, 2014)
[4] Christine I.Podilchuk and Edward J. Delp (2001). Digital watermarking algorithms and applications.IEEE: Signal Processing (http://www.symantec.com/about/profile/antipiracy/)
[5] Mitsuo Okada (2012). Privacy-Secure Digital Watermarking for Fair Content Trading. Kyoto University, Japan
[6] (http://www.oracle.com).