Dual Watermarking in Cyber Security

Mrs.A. Lakshmi Priya[1], Dr.S. Letitia[2]
Associate professor, Department of ECE, Global Institute of Engineering and Technology, Vellore, India
a.v.lakshmipriyaa@gmail.com
Dr. S. Letitia, Thanthai Periyar Government Inst. Of Engg. And Technology, Vellore, India
letitiedurai@gmail.com

ABSTRACT

Cyber security is generally a conservatory of the conventional information system security that is aimed at protecting cyber threats, like cyber terrorism, cyber warfare, and cyber espionage to corrupt digital information. This leads to increase the researches in cyber security. This paper proposes the application of dual watermarking in cyber technology, focusing on forgery detection. The rest of the paper presents a brief overview of cyber security and the role of digital dual watermarking.

Keywords

Dual watermarking, Cyber security and Cyber Technology

INTRODUCTION

Cyber security is the progression and practices deliberate to shield network, program and data from attacks, unauthorized access. All illegal acts breaches computer security is referred as computer crimes or cyber crimes. The technology that protects the information and systems from cyber threats like malware injection and stealing of data via the internet is known as cyber technology. Most of the cyber threats are aiming secret, political, military and infrastructural assets of a nation or people. Further the cyber attacks refers to deliberate action, perhaps an extended period of time to alter, disrupt, deceive, degrade or destroy adversary computer system or network or information. Among that one of the most increasing threats is Identity theft.[1]

Identity theft overview

Identity theft refers acquiring personal data or identity of known or unknown person in order to gain benefits to convict another person. Where Identity thieves are constantly sprouting and discovering new ways to encompass the owner's information. In most of the identity theft is obtained, by acquiring personal and financial information of the owner and use it to act in the same name. Some of the Identity thefts are Social security fraud, Driver's license fraud, Criminal identity theft, financial identity theft, change of address fraud, employment identity theft, Peer-to-peer attacks, medical identity theft and creation of new person. [2][3]

Social security fraud : Stealing the social security number of a person to make unauthorised purchases or to receive welfare payments illegally through credit cards.

Driver's license fraud : Issuing the driver's license to others using owners identity. This leads to suspending or revoking the license of the owner.

Criminal identity theft : Most serious type of identity theft, where criminals uses identification of others information to escape.

Financial identity theft : Most of the peoples associated with this form of crime, this involves stealing the owners personal information through viruses to create fake account like checking account, credit card, car loans and mortgages.

Change of address fraud : Changing the mailing address the thief can able to divert all mails to an alternate mail address.

Employment identity theft : Criminals and illegal immigrants are stealing others identity to avoid their real, personal history checks.

Peer-to-peer attacks : Using peer-to-peer services thieves delivers Trojan horse attacks to user and trying to access their computer to obtain password and other personal information.

Medical identity theft : Using others information while receiving medical care to avoid payments.

Creation of new person : Combining all information they have stolen from multiple victims and crating new identity.

The various types of identity theft and percentage based on Federal Trade Commission's Consumer Sentinel Network in year 2015 is shown in fig(1).[2]

DOI : 10.24297/jac.v13i10.5834

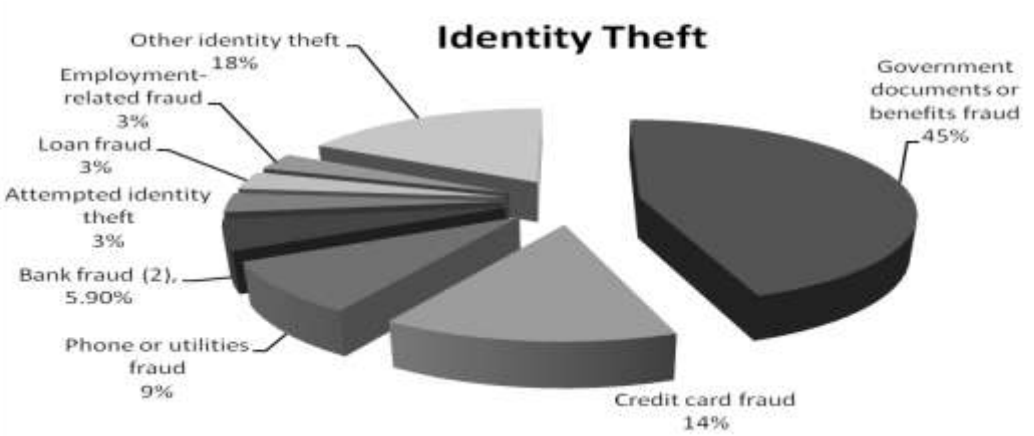

Fig 1: Types of Identity theft and its occurrence in percentage

The number of data breaches and records exposed, 2006-2016 based on cyber crime report is shown in fig(2)

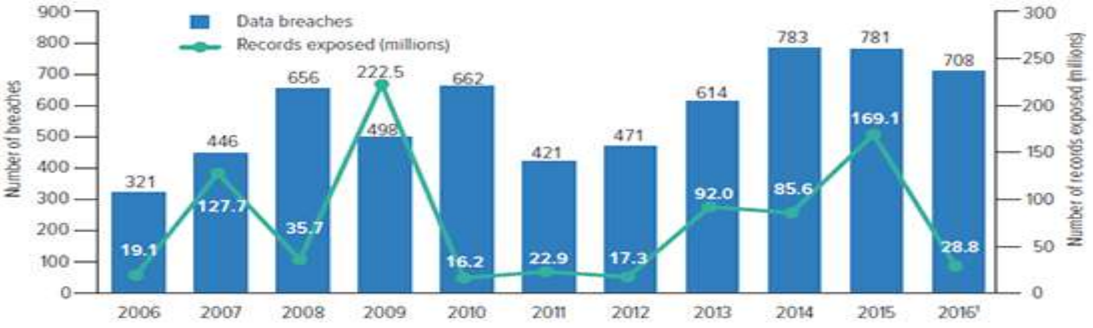

Fig 2: statistics 2016 (from www.idtheftauthority.com; cyber complaints as on sep 2017)

Identity thieves encroaches the victim’s right to personal dignity by spoiling the owner’s honour and reputation and causing incessant arousing stress, due to the reality that theft of confident personal data can be inherent. These threads are not only local but also global in nature, and targets all technologies like software, service providers and consumers, private and public sectors. As long as these are connected with internet there is wide change of exposing to cybercrime.[3]

DIGITAL WATERMARKING

Digital watermarking technology has flounce up the attention of the researches to equip a standard resolution to illegal copying, meddling, editing and manipulating the owner’s information. This fact, together with the exponential increase of computer leads to ease the distribution of multimedia content and these data can be easily duplicated and distributed without the owner’s permission. In recent years, there has been dramatic increase in copying and sharing patented contents and due to peer-to-peer sharing system it becomes more complex. Digital watermarking gives the standard solution to prove ownership authentication and copyright protection.[4] This analysis will focus on digital watermarking application in cyber security to refine cyber technology in order to reduce cyber crimes.

PREVIOUS WORKS

Agbaje, M.O, Awodele O., and Ogbonna A.C (2015) proposed the application of Digital watermarking to cyber security and gives a brief overview about cyber security and the detailed report of crimes and there statistics. The focus on digital watermark and to examine all its probable cyber security application. Also states the importance of cyber security in developing countries to roll out cyber crimes.

Braun (2014) offered a Forensic evidence of copyright infringement by Digital Audio Sampling Analysis - Identification. They present the methods of audio analysis including the use of watermarking.

Harjito (2013) proposed copyright protection of scalar and multimedia sensor network data using digital watermarking. This article examines different watermarking algorithm to deal with the concern of copyright protection of scalar data in wireless sensor networks and image data in wireless multimedia sensor network, to facilitate the proprietorship information remnants safe along with the sensor nodes.

Topkara (2005) projected a watermarking based approach, and its implementation for mitigating against phishing attacks-a form of web based identity theft (ViWiD). ViWiD is an integrity test apparatus based on visible watermarking of logo images. Every user is using a unique watermark to share secret between the company the user in order to avoid “one size fits all attacks".

Prakobphol and Zhan (2002) suggested the design and prototype implementation of an image veri-fication server that employs digital watermarking to thwart fraudsters from fake legitimate us-er's contour in social networks using the image saved from the networks. The watermark algorithm is realized in the Discrete Wavelet Transform.

DIGITAL WATERMARKING IN IDENTITY THEFT

(i) **Data integrity:** The reliability of digital records like ownership authentication and attribution are the vital areas in Digital integrity.

(ii) **Privacy**: Privacy related to the records and confined information.

(iii) **Data security:** The purpose of digital watermarking is to improve the robustness to attacks by embedding additional information in the existing content. With this information the author, the ownership or other maintained features of the manuscript may be demonstrated. [1]

DUAL WATERMARKING

Dual watermarking caters a coherent way to two major security concerns: Information recovery and ownership identification. To resolve ownership authentication a unique attributes such as fingerprint, retina scans or DNA structures can be used as primary watermark and user precise indispensable information can be used as secondary watermark. In practice most of the researchers carried out in dual watermarking, one among the watermarks is visible and another is invisible. The secondary watermark is rooted into the primary watermark and the resultant watermark is embedded in the source image. Similarly the primary watermark is extracted and compared with the original watermark based on some similarity measures if it meets the desired threshold then the algorithm permits to retrieve the secondary watermark. If both the watermarks are reterived back with best similarity measure then the source image or document is permitted to make the changes in it.[5]

Dual Watermarking in Identity Theft

The data security of the information by the author, the ownership or other maintained features of the manuscript is increased by employing dual watermarking. This protects the manuscripts against illegal copying and manipulating the digital content without the knowledge of the owner. Here we propose dual watermarking where both the watermarks are invisible. This will increase the computational efficiency of the document further. This will reduce the most common identity thefts like financial identity theft and criminal identity theft caused by technical or non-technical methods. Maximum of such theft are occurred on database where the data are accessed directly and moderately while transmitting the data and also posibily when the documents are being scaned. Example, Let the ID of a person is scanned to determine authenticity then digital watermark protects the ID from altering, regenerating, photo swaping and counterfeiting. This can also enable cross-jurisdictional authentication, automates document authentication, provides forensic tracking and also provides compatibility with both new and existing ID design.[1][5]

EMBEDDING AND EXTRACTION ALGORITHM AGAINST IDENTITY THEFT

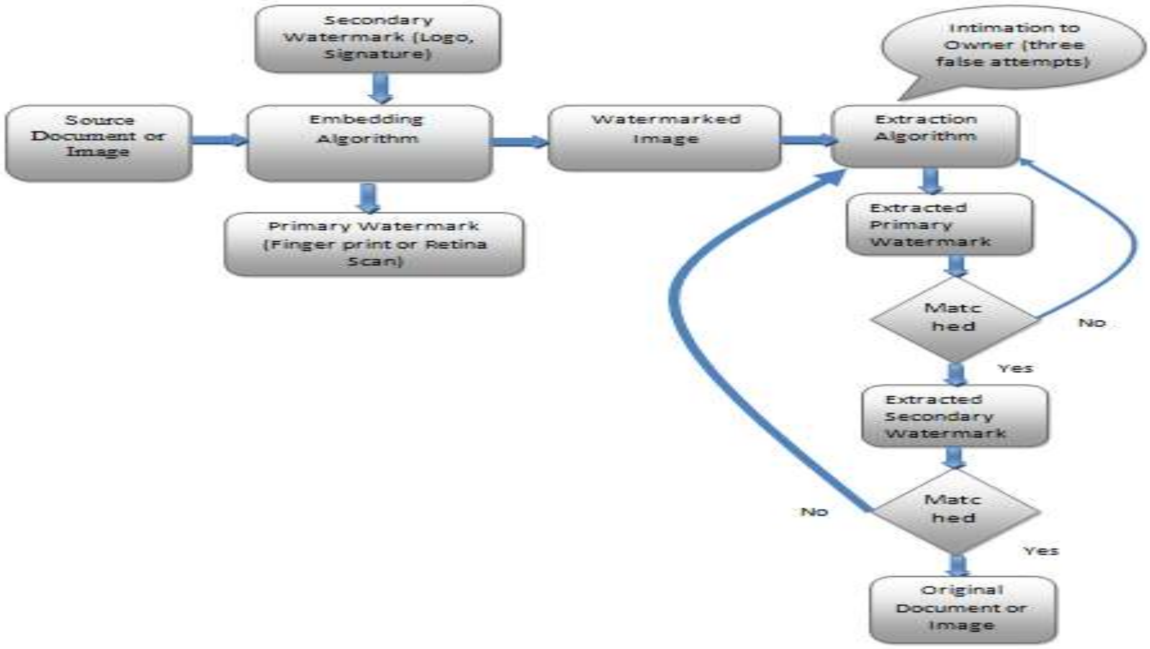
Secondary Watermark (Logo, Signature)
Source Document or Image
Embedding Algorithm
Primary Watermark (Finger print or Retina Scan)
Watermarked Image
Intimation to Owner (three false attempts)
Extraction Algorithm
Extracted Primary Watermark
Matc hed
No
Yes
Extracted Secondary Watermark
No
Matc hed
Yes
Original Document or Image

Fig 3. Embedding and extraction process

Figure 3 shows the proposed algorithm for embedding and extracting the watermark using identity for the management scheme. In embedding algorithm the sourse document or image of the owner is embedded with two watermarks among which one is owner specific unique watermark along with some user specific information. If both the watermarks are retrived back the source document or image can be modified. Not more than three attemps are permitted to access the source if fails then the information is passed to the owner with immediate effect that some one is try to hack there personal information.

APPLICATIONS

Mainly used in ID Security, authentication and piracy deterrent, Dual watermarking is used to protect and identify the documents against alteration, regeneration, photo swapping and counterfeiting. This enables cross-jurisdictional endorsement without standard ID design also automates document authentication. This also provides forensic analysis and tracking and cpmpatibility with new and existing ID designs.

CONCLUSION

Cybercrime and cyber security issues are hardly separated in an interrelated environment. Cyber security plays an vital role in the fragmentary development of information technology and also in Internet services. Enhancing cyber security by safe guarding critical informations structures are most essential to each and every nation's security and economic welfare. The proposed dual watermarking in cyber security algorithm can be varied depending on the type of application for services being rendered. This helps people to recognize cyber watermarking that is watermarking in cyber security and its importance. All developing countries need to integrate such type of protection measures in Internet from the beginning. This might initially increase the cost of Internet services, but in long-term measures it will avoids the costs and damages imposed by cybercrime are large and far overshadow any initial expenditure on technical fortification measures and network uphold.

REFERENCES

1. Agbaje M.O, Awodele O., and Ogbonna A.C. 2015. "Application of Digital Watermarking to Cyber Security (Cyber Watermarking)", Proceedings of Information Science & IT Education Conference.
2. Types of Cyber attacks. Reterived from www.google.co.in
3. Overview of different types of Identity Theft. 2015. Retrived from www.idtheftauthority.com
4. Lakshmi priya. A, Letitis.S.2015,"Copyright protection for Digital Colour Images in RGB plane using Improved DWT-DCT-SVD Algorithm", International joural of applied Engineering Research.
5. Lakshmi priya. A, S. Letitia. 2016. "Copyright protection of Dual Color Images Based on Singular Valuue Decomposition Using Improved Arnold", Asian Journal of Information Technology.
6. Accenture. 2010. *Cyber security: An escalating global challenge for all organizations*.Alexander, A. (2015). *Protecting yourself from identity theft*. Retrieved from www.thewatermarkgrp.com
7. Braun, S. K.. 2014. Forensic evidence of copyright infringement by digital audio sampling analysis identification marking. International Journal of Cyber-Security and Digital Forensics (IJCSDF), 3(3), 170-182.
8. Prakobphol. K., Zhan, 2002. Alleviating identity theft in social networks
9. Topkara. M., Ashish. K., Mikhail. J.A. and Cristina. N. 2005, "ViwiD: Visible watermarking based defence against phishing", Digital watermarking lecture notes in Computer seience.
10. Cox, J., Miller, M. L., Bloom, J. A., Fridrich, J., & Kalker, T. 2008. Digital watermarking and steganography.Elsevier Inc.
11. IBM. 2014 . IBM Security Services 2014 Cyber Security Intelligence Index Analysis of cyber attack and incident data from IBM's worldwide security operations.
12. Information commissioner. 2010. *Guidelines for preventing identity theft*. Retrieved from www.ip-rs.si

DOI : 10.24297/jac.v13i10.5834