File System Security for Internal Organization Using Certified Authority

Shubham Kumbhar[1], Sohel Inamdar[2], Shaharukh Pattekari[3] , Satish Narhe[4]

[1234]Department of Computer Engineering , Indira College Of Engineering and Management, Pune

---***---

Abstract - *Rapid increase in E-commerce website leads to some serious security issues, so secure payment system must be implemented. This paper presents a replacement approach for providing limited data solely that's necessary for fund transfer during online shopping thereby safeguarding client information and increasing client confidence and preventing fraud. The method uses Image steganography for this purpose. Method introduce a certified authority (CA) for identity checking of customer, CA consist a copy of image in which data is hidden, another copy is distributed to customer. Single copy has no meaning in transaction as image is divided into two parts, Therefore, provides security in online payment system. Encryption algorithm is being used for unique information enciphering. The outcome of the encryption algorithm is structured into various equally distributed blocks. In steganography, secret cipher blocks are assigned to carrier image for data inserting by mapping mechanism using breadth first search*

***Key Words*: Image Segmentation, Encryption, Decryption, Certified Authority, Steganography**

1. INTRODUCTION

With the increasing amount of mobile devices and web services, users can access their personal accounts to send confidential business emails, upload photos to albums in the cloud or remit money from their e-bank account anytime and anywhere. While logging into these services in public, they may expose their passwords to unknown parties unconsciously. People with malicious intent could watch the whole authentication procedure through omnipresent video cameras and surveillance equipment, or even a reflected image on a window. Once the attacker obtains the password, they could access personal accounts and that would definitely pose a great threat to ones assets. Shoulder surfing attacks have gained more and more attention in the past decade.

2. LITERATURE SURVEY

An Online shopping is the retrieval of product information via the Internet and issue of purchase order through electronic purchase request, filling of credit or debit card information and shipping of product by mail order or home delivery by courier . Identity theft and phishing are the common dangers of online shopping. Identity theft is the stealing of someone's identity in the form of personal information and misuse of that information for making purchase and opening of bank accounts or arranging credit cards. In 2012 consumer information was misused for an average of 48 days as a result of identity theft . Phishing is a criminal mechanism that employs both social engineering and technical subterfuge to steal consumers personal identity data and financial account credentials. In 2nd quarter of 2013, Payment Service, Financial and Retail Service are the most targeted industrial sectors of phishing attacks . Secure Socket Layer (SSL) encryption prevents the interception of consumer information in transit between the consumer and the online merchant. However, one must still trust merchant and its employees not to use consumer information for their own purchases and not to sell the information to others. [1]

This letter presents a novel steganography scheme capable of concealing a piece of critical information in a host message which is a binary image (e.g., a facsimile). A binary matrix and a weight matrix are used as secret keys to protect the hidden information. Given a host image of size(m*n) , the proposed scheme can conceal as many as log2(mn + 1) bits of data in the image by changing, at most, two bits in the host image. This scheme can provide a higher security, embed more information, and maintain a higher quality of the host image than available schemes. [2]

With the development of the Internet, online shopping as a consumer fashion, gradually become a popular shopping channel for consumers. From the China Internet Network Information Center data show that: in 2009 China's online shopping market transaction size of 2,500 million, representing a doubling in 2008. In 2010 market size of online shopping will be over 430 billion yuan. Online shopping population is also substantial growth in 2009, bought online at least once a number of historic Chinese netizens exceeded 100 million people, reaching 108 million, an increase of 46 Percent. And in 2010, used the online shopping of Internet users is nearly 2 million people. Online shopping has become the fastest growing and most relevant to the interests of users of network applications. At this stage, consumers take online store, online store and online auction model of online shopping, it is a new personal consumption patterns.[3]

Steganography is an ancient art. With the advent of computers, we have vast accessible bodies of data in which to hide information, and increasingly sophisticated techniques with which to analyze and recover that information. While much of the recent research in steganography has been centered on hiding data in images, many of the solutions that work for images are more complicated when applied to natural language text as a cover medium. Many approaches to steganalysis attempt to detect statistical anomalies in cover data which predict the presence of hidden information. Natural language cover texts must not only pass the statistical muster of automatic analysis, but also the minds of human readers. Linguistically nave approaches to the problem use statistical frequency of letter combinations or random dictionary words to encode information. More sophisticated approaches use context-free grammars to generate syntactically correct cover text which mimics the syntax of natural text. None of these uses meaning as a basis for generation, and little attention is paid to the semantic cohesiveness of a whole text as a data point for statistical attack.[4]

3. METHODOLOGY

Algorithms or methodology are as Follows:

A. Blowfish Algorithm

Blowfish is an encryption algorithm that can be used as a replacement for the DES or IDEA algorithms. It is a symmetric (that is, a secret or private key) block cipher that uses a variable-length key, from 32 bits to 448 bits, making it useful for both domestic and exportable use. Schneier designed Blowfish as a general-purpose algorithm, intended as an alternative to the aging DES and free of the problems and constraints associated with other algorithms. At the time Blowfish was released, many other designs were proprietary, encumbered by patents or were commercial or government secrets. Schneier has stated that, ”Blowfish is unpatented, and will remain so in all countries. The algorithm is hereby placed in the public domain, and can be freely used by anyone.”

B. Image Steganography

Image Steganography In Image Steganography we use LSB Technique to hide data in image bit by bit . In these technique every pixel of image having RGB format bit And there LSB(Least Significant Bit) are useless for our image. so we place our data bit by bit in every LSB bit of RGB Pixel .

C. Binary search algorithm

Searching algorithm will be used for searching the similar products from the entire site with respect to the item which user have selected. The binary search algorithm begins by comparing the target value to the value of the middle element of the sorted array. If the target value is equal to the middle element’s value, then the position is returned and the search is finished. If the target value is less than the middle element’s value, then the search continues on the lower half of the array; or if the target value is greater than the middle element’s value, then the search continues on the upper half of the array. This process continues, eliminating half of the elements, and comparing the target value to the value of the middle element of the remaining elements - until the target value is either found (and its associated element position is returned), or until the entire array has been searched (and ”not found” is returned).

D. Bubble Sort

sometimes referred to as sinking sort, is a simple sorting algorithm that repeatedly steps through the list to be sorted, compares each pair of adjacent items and swaps them if they are in the wrong order. The pass through the list is repeated until no swaps are needed, which indicates that the list is sorted. The algorithm, which is a comparison sort, is named for the way smaller elements ”bubble” to the top of the list. Although the algorithm is simple, it is too slow and impractical for most problems even when compared to insertion sort. It can be practical if the input is usually in sort order but may occasionally have some out-of-order elements nearly in position

3. ARCHITECTURE

Proposed System describes encryption and decryption technique and provide security to data which is transfer over the network.

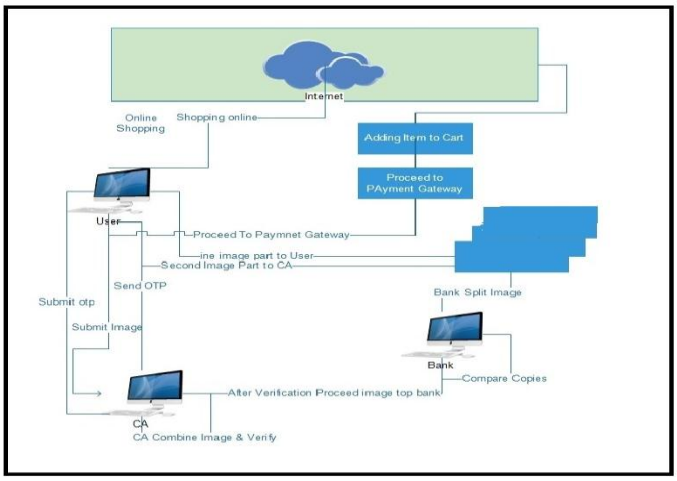

Fig 1: System Architecture

4. MATHEMATICAL MODEL

System Description

Let S be the system,

S ={ T_b, X, F, b, E_m, b_c, CA, C_{ch}, phi_F }

T_b= File Chunk size/block size of block

X= Encryption key

F= Data owner's file targeted for encryption

Input:

F={b_1,b_2,b_3,....,B_m }

b=File chunk/block

b=(c_1,c_2,c_3,....,|b|)

E_m=Encoding map for every character

b_c= Binary equivalant of character c

CA= Circular vector of character

C_{ch}= Cipher text for character for ch

Output:

C_{ch}=\{e_1,e_2,e_3,......|e_b|

phi_F=Size of File

Success: Data encrypted and key generate

Failure: Bit conversion problem, data outsourcing detection problem.

5. CONCLUSION

In this project, a payment system is applied for E-Commerce for online shopping. It is proposed by combining visual cryptography and image based Steganography, It provides confidentiality for customer data and stops misuse of data at merchants side. The method is concerned with avoidance of identity theft and customer data confidence. In comparison to other banking application which uses Visual cryptography and Steganography, basically applies for physical banking, the suggested method can be practically used for E-Commerce by focusing on payment during online shopping as well as physical banking

6. REFERENCES

[1] Souvik Roy and P. Venkateswaran, Online Payment System is using Steganography and Visual Cryptography, IEEE Students Conference on Electrical, Electronics and Computer Science 2014

[2] Yu-Chee Tseng,Yu-Yuan Chen, and Hsiang-Kuang Pan, A Secure Data Hiding Scheme for Binary Images, IEEE TRANSACTIONS ON COMMUNICATIONS, VOL. 50, NO. 8, AUGUST 2002

[3] Jihui Chen, XiaoyaoXie, and Fengxuan Jing, The security of shopping online, Proceedings of 2011 International Conference on Electronic and Mechanical Engineering and Information Technology (EMEIT), vol. 9

[4] K. Bennet, Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding information in Text, Purdue University, Series Tech Report 2004 2013

[5] J.C. Judge, Steganography: Past, Present, Future, SANS Institute, November 30, 2001

[6] M. Naor and A. Shamir, Visual cryptography , Advances in Cryptography: EUROCRYPT 94, LNCS, vol. 950, pp. 112, 1995.

[7] Harshad Talera,Nalini Wagaskar,Shital Kapse,Pooja Deshmukh,Shweta Shanwad, Advanced Secure Online Payment using Stegano Images, International Engineering Research Journal (IERJ), Volume 2 Issue 5 Page 1908-1910, 2016 ISSN 2395-1621