Survey on shopping recommendation system with secure online payment

Ajay Mangaj[1], Aditya Chavan[2], Pritesh Joshi[3], Priti Mithari[4]

Department of Computer Engineering, Pune University, India[1,2,3,4]

Abstract: Recommendation System is used to recommending to the user. The objective of recommender to assist users to find out items which they would be interested in. However, current ways suffering from such issues as information poorness, recommendation quality, and big error in predictions. The paper tends to take ideas of object normality from psychology and gives a unique Typicality-based Collaborative filtering recommended technique named TyCo. A defining feature of normality-based Collaborative filtering is that it finds "neighbors" of users supported user typicality grouped in user teams. E-commerce market is growing rapidly in last 5 years. The ever increasing quality of online searching, Debit or MasterCard fraud and private data security area unit major issues for patrons, merchants and banks especially within the case of situation where Card Not Present. The paper gives an idea about the shopping recommendation with filtering methods and online payment gateway system using steganography.

Keywords: Steganography, Online shopping, E-Commerce, Encryption.

I. INTRODUCTION

In extremely increasing E-Commerce market setting, online searching has grown up in quality over the years, primarily as a result of folks notice it convenient and simple to discount, search from the comfort of their home or workplace. During this paper, we tend to area unit specializing in security of customer's personal data throughout on-line searching. On-line searching may be a style of electronic commerce that permits customers to directly get merchandise or services from a vendor over the net employing a browser.

Steganography is the art of concealing a file, message, image, or video inside another file, message, image, or video [4].The good thing about Steganography over cryptography is that the supposed secret message doesn't attract attention to itself as an object of Examination. Plainly visible encrypted messages—no matter how much unbreakable—arouse interest, and should in themselves be incriminatory in countries wherever cryptography is prohibited. Thus, whereas cryptography is the art of protecting the contents of a message alone, Steganography is bothered with concealing the very fact that a secret message is being sent, moreover as concealing the contents of the message.

Encryption is that the method of cryptography messages or data in such the way that solely approved parties will browse it. The supposed communication, data or message, remarked as plaintext, is encrypted mistreatment associate degree secret writing formula, generating cipher text which will solely be browse if decrypted. associate degree secret writing theme sometimes uses pseudo-random secret writing key generated by associate degree formula [2].

Electronic commerce is commerce in merchandise or services mistreatment laptop networks, like the net. Electronic commerce attracts on technologies like mobile E-commerce, electronic funds transfer, provide chain management; web selling, on-line dealing process, Electronic knowledge Interchange (EDI), inventory management systems, and automatic knowledge assortment systems [4].The Major Problems in online shopping are Identity theft and phishing. Identity theft is that the crime of getting the private or money info of another person for the only purpose of forward that person's name or identity so as to form transactions or purchases or the fallacious observe of mistreatment another person's name and private info so as to get credit, loans, etc. [6]. Example- In 2010, 7.0% of social unit within the U.S. had a minimum of one member expertise fraud. At about 8.6 million households, 7.0% aren't any tiny threat, thus it's vital to remain on your toes once it involves Information security. Phishing is used to acquire sensitive data like usernames, passwords and MasterCard details (generally, indirectly, money), typically for malicious reasons, by masquerading as a trustworthy entity in associate transmission [2] [3]. Phishing email can generally direct the user to go to a web site wherever they're asked to update personal data, like an Arcanum, MasterCard, Social Security, or Checking account numbers that the legitimate organization already has. Phishers area unit targeting the shoppers of banks and on-line payment services. Emails, purportedly from the inner Revenue Service, are accustomed reap sensitive knowledge from U.S. taxpayers. Recent analysis has shown that phishers could in theory be ready to confirm that banks potential victims use and target imitative emails consequently.

Providing a new method which uses steganography and visual cryptography based on text [7], i.e. text-based Steganography that decreases the sharing of information between consumer and online merchantman but empower successful fund transfer from the consumer's account to merchantman's account by protecting customers personal information and anticipating misuse of information from merchants end. Paper provided a new idea by introducing

an Image Steganography and cryptography techniques to provide security to customer's transaction details [2]. The previous transaction history of customer is used to provide a product recommendation [1].

This Survey paper is organized as follows: Section 2 Gives brief explanation of related work.Explains secure online payment technologies in Section 3. Section 4 concludes the paper.

II. RELATED WORK

A. Steganography

Section presents a brief survey of related work in the area of banking security based on Image Steganography and visual cryptography [9]. A customer authentication system using visual cryptography but it is specially designed for physical banking [9].A signature based authentication system for core banking is but it also requires physical presence of the customer presenting the share. Proposed combined image based steganography and visual cryptography authentication system is used for customer authentication in core banking is proposed [8]. A message authentication image algorithm is proposed into protect against e-banking fraud. A biometrics in conjunction with visual cryptography which is used as authentication system .By studying all these papers we came to conclusion of using Image Steganography and cryptography.Steganography is the method of concealing messages or information within other non-secret text or data or hiding of a secret message within a normal message and the extraction of it at its destination or maybe is the practice of concealing a file, message, Text [4], image [5], audio [6], or video within another file, message, image, or video.

Text Steganography

Using text based Steganography, the message remains hidden. For hiding this message various methods are used like shifting the word and line, in open spaces, in word sequence .Various other methods are also used like Properties of a sentence. These are also used to hide secret messages such as number of words, number of characters, number of vowels, and position of vowels in a word. There are various advantages of choosing text steganography on behalf of other Steganography techniques. First, is it requires smaller memory and second is communication becomes simpler using Text based Steganography techniques [1]. But Drawback of this method is that it is a complex method of sentence formation. In the result, for hiding for letter word we require 8 words. So if we want to hide a large message, large no of words are required that will create a complexity in sentence construction. So, we use Image Steganography and cryptography. Image Steganography is method of Concealing messages within the lowest bits of noisy images. The advantages are that the hidden text will not in focus. It can be passed in innocuous content like an image. [2] By making some slight changes to colour values, for example, you can exchange some bits that are practically undetectable. Visual Cryptography (VC) is proposed by MoniNaor and Adi Shamir, in 1994 [10].

Video Steganography

Video steganography is very important to transmit the important data like banking and military information in a protected manner. It is the process of hiding some secret information inside a video. The addition of this information to the video is not identifiable by the human eye as the change of a pixel color is insignificant. The projected methodology creates an index for the key info and also the index is placed in a very frame of the video itself. With the assistance of this index, the frames containing the key info ar placed. Hence, throughout the extraction method, rather than analysing the whole video, the frames covering the key knowledge are analysed with the assistance of the index at the receiving end. Using steganography method the possibility of finding the hidden information by an attacker is lesser when compared to the normal technique of hiding information frame by frame in a sequential manner. It also decreases the computational time taken for the extraction process [2] [3].

Audio Steganography

Audio Steganography it is a method used to transfer hidden info by altering an audio signal in an unnoticeable manner. The science of concealing some secret text or audio data in a very host message. The host message before steganography and also the steno message after steganography have identical characteristics. Embedding secret messages in digital sound are a more difficult process. Varieties of techniques for embedding information in digital audio have been established. This paper presents a comprehensive survey of some of the audio steganography methods for data hiding. Least Significant Bit (LSB) technique is one of the simplest approaches for secure data transfer. In this paper different data hiding method used to protect the information are discussed. Audio data hiding is one of the most effective ways to protect the privacy [2] [3].

Visual cryptography

Visual cryptography is a cryptographicprocedure which permits visual information (pictures, text, etc.) to be encrypted in such a technique that decryption converts a mechanical process that does not require a computer. One of the best-known techniques has been credited by Adi Shamir and MoniNaor, who developed it in 1994.[1] They demonstrated a graphicsecret sharingstructure, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any $n - 1$ parts revealed no information about the original image. Each share was printed on a distinct transparency, and decryption was done by overlaying the shares. When all $n$sharewas overlaid, the original image would appear. There are several simplifications of the basic system, including k-out-of-n visual cryptography [2][3].

Encryption

Encryption is the procedure of converting plain text data (plaintext) into approximately that appears to be random and worthless (cipher text). Decryption is the process of

translating cipher text back to plaintext. To encrypt more than a small quantity of data, symmetric encryption is used. A symmetric key is used during both the encryption and decryption processes. To decrypt a specific piece of cipher text, the key that was used to encrypt the data must be used [3].

B. Recommender Systems

Now-a-days there have been many works on recommender systems and most of these works focus on developing new methods of recommending items to users the objective of recommender systems is to assist users to find out items which they would be interested in.Currently, recommendation methods are mainly classified into hybrid methods,content based (CB),collaborative filtering (CF)[2]. For the reason that we are concentrating on suggesting a new CFmethod, we will present the related works about CFmethods in more details.

Content-Based Recommender Systems

Content-Based Recommender Systems of such kind of recommendation methods comes from the fact that people had their subjective assessments on some items in the past and will have the similar assessments on other similar items in the future. The descriptions of items are examined to identify fascinating items for users in CB recommender systems. Based on the items a user has rated, a CB recommender learns a summary of the user's preferences or user's interests. According to a user's interest summary, the items which are comparable to the ones that the user has rated highly in the past or preferred will be recommended to the user. For CB recommender systems, it is vital to learn users' profiles. Various learning approaches have been applied to construct profiles of users.

Collaborative Filtering

Collaborative filtering recommendation methods predict the likings of active users on items based on the preferences of other items or similar users. There are two kinds of CF methods, namely item-based CF approach and user-based CF approach. The basic idea of user-based CF approach is to provide reference of an item for a user based on the views of other like-minded users on that item. The user. The basic idea of item-based CF approach is to provide a user with the reference of an item based on the. The user-based CF, the item-based CF approach first finds out a set of nearest "neighbors" (similarly items) for each item.

The item based CF recommender systems try to predict a user's ranking on an item based on the ratings given by the user on the neighbors of the target item. For each user-oriented collaborative Filtering and item-oriented collaborative Filtering, the measuring of similarity between users or things could be a vital step. Pearson correlation coefficient, cosine-based similarity, vector house similarity, so on is wide utilized in association measuring in CF strategies. Combining externally specified aggregate ratings information in CF methods.

Hybrid Recommender

Hybrid Recommender Systems are a combination of collaboration and content based methods, so as to help avoid some limitations of content-based and collaborative systems. Naive hybrid approach is to implement collaborative and CB methods separately, and then combines their predictions by a combining function, such as a linear combination of ratings or a voting scheme or other metrics. Some hybrid recommender systems combine item-based CF and user-based CF.

III. TECHNOLOGIES USED

A. Least Significant Bit

Least significant bit (LSB) insertion could be a common, straightforward approach to embedding data in an exceedingly cowl image. the smallest amount vital bit (in alternative words, the eighth bit) of some or all of the bytes in a picture is modified to slightly of the key message. once employing a 24-bit image, slightly of every of the red, green and blue color elements will be used, since they're every described by a computer memory unit. In alternative words, one will store three bits in every element. associate 800×600 element image, will so store a complete quantity of 1,440,000 bits or 180,000 bytes of embedded information. as an example a grid of three pixels of a 24-bit image will be as follows:

For Example:

(00101101 00011100 11011100)

(10100110 11000100 00001100)

(11010010 10101101 01100011)

When the amount 200, that binary illustration is 11001000,is embedded into the smallest amount significant bits, this a part of the image, the ensuing grid is as follows:

(0010110**1** 0001110**1** 1101110**0**)

(1010011**0** 1100010**1** 0000110**0**)

(1101001**0** 1010110**0** 01100011)

Although the amount was embedded into the primary eight bytes of the grid, solely the three underlined bits required to be modified in step with the embedded message.

B. RC6

RC6 (Rivest Cipher 6) could be a symmetric key block cipher derived from RC5.RC6 correct encompasses a block size of 128 bits and supports key sizes of 128,then 192, and 256 bits, but, like RC5, it should be parameterized to support a good sort of word-lengths, key sizes, and variety of rounds. RC6 is extremely almost like RC5 in structure, victimization data-dependent rotations, standard addition, and XOR operations; indeed, RC6 can be viewed as interweaving 2 parallel RC5 encoding processes, however, RC6 will use an additional multiplication operation not gift in RC5 so as to form the

rotation depends on equally in an exceedingly word, and not simply the smallest amount important few bits.

C. One Time Password(OTP)

A one-time password (OTP) is a keyword that is effective for only one login session or operation, on a computer system or other numerical device. OTPs avoid a number of shortcomings that are associated with traditional (static) password-based authentication; a number of implementations also include two factor authentication by confirming that the one-time password requires access to somewhat a person has (such as a small keying fob device with the OTP calculator built into it, or a smart card or exact cellophane) as well as somewhat a person knows (such as a PIN).

The most important advantage that's self-addressed by OTPs is that, in distinction to static passwords, they're not prone to replay attacks. this implies that a possibleinterloper who manages to record an OTP that was already wont to log into a service or to conduct a dealing will not be able to abuse it, since it will not be valid.. A second major advantage is that a user who uses an equivalent (or similar) positive identification for multiple systems, isn't created prone to all of them, if the positive identification for one amongst these is gained by an offender. variety of OTP systems additionally aim to substantiate that a session cannot simply be interrupted or derived while not data of random knowledge created throughout the previous session, so reducing the attack surface more. ways of delivering OTP area unit text electronic messaging, mobile, exclusive token, web based mostly technique, hard copy.

IV. CONCLUSION

In this paper, 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 merchant's 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.

ACKNOWLEDGEMENT

REFERENCES

[1] Yi CAI, Ho-Fung Leung, Qing Li, Huaqing Min, Jie Tang, and Juanzi Li, "*Typicality-Based Collaborative Filtering Recommendation*", IEEE Transactions On Knowledge And Data Engineering, Vol. 26, No. 3, March 2014.

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

[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, Pp. 4693-4696, 2011.

[4] "*Suspicious emails and Identity Theft*", *Internal Revenue Service*. Archived from the original on 2011-01-31, Retrieved July 5, 2006.

[5] Walter Bender, Daniel Gruhl, Norishige Morimoto, A. Lu, "*Techniques for Data Hiding", IBM Systems Journal*, Vol. 35, Nos. 3 & 4, pp. 313- 336, 1996.

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

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

[8] M. Naor and A. Shamir, "*Visual cryptography*", Advances in Cryptography: EUROCRYPT'94, LNCS, vol. 950, pp. 1–12, 1995.

[9] S.Premkumar, A.E.Narayanan, "*New Visual Steganography Scheme for Secure Banking Application*", Proceeding of 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET), pp. 1013 – 1016, Kumaracoil, India, 2012.

[10] KalavathiAlla, Dr. R. Siva Rama Prasad, "*An Evolution of Hindi Text Steganography*", Proceeding of Sixth International Conference on Information Technology, pp. 1577-1578, Las Vegas, NV, 2009.