

International Journal of Computer Science and Mobile Computing



A Monthly Journal of Computer Science and Information Technology

ISSN 2320-088X

IJCSMC, Vol. 4, Issue. 1, January 2015, pg.532 – 538

RESEARCH ARTICLE

Secure E-marketing Using Steganography & Emergence of Cryptography

Sana Shiva, M.Tech CSE from Brilliant Institute of Engineering & Technology
A.Hari Teja, Associate Professor at Brilliant Institute of Engineering & Technology

Abstract - Traditional selling goods is possible to do electronically because of certain software programs that run the main functions of an E-commerce including product display online ordering and inventory management. E-commerce includes business activities that are business-to-business extended enterprise computing because it assists companies with many levels of current business transactions as well as creating a new online business opportunities that are global in nature. Increasing popularity of online shopping Debit or Credit card fraud and personal information security concerns for customers and merchants specifically when card is not present, our analysis presents limited information only that is necessary for fund transfer during online shopping. Compare to existing the proposed algorithm combined the application of steganography and visual cryptography increasing customer confidence and preventing identity.

Keywords – Cryptography, Steganography, E-commerce, Bit plane.

1. Introduction:

Steganography is the art of hiding communication, steganographic system thus embeds hidden content in unremarkable cover media so as not to arouse an eavesdropper's suspicion. In the past, people used hidden tattoos or invisible ink to convey steganographic content. Today, computer network technologies provide easy-to-use communication channels for steganography. Essentially, the information-hiding process in a steganographic system starts by identifying a cover medium's redundant bits that can be modified without destroying that medium's integrity. The embedding process creates a stego medium by replacing these redundant bits with data from the hidden message. Modern steganography's goal is to keep its mere presence undetectable, but steganographic systems because of their invasive nature leave behind detectable traces in the cover medium. Even if secret content is not revealed, the existence of it is modifying the cover

medium changes its statistical properties, so eavesdroppers can detect the distortions in the resulting stego medium's statistical properties. The process of finding these distortions is called statistical steganalysis.

Cryptography is the science of writing in secret code and is an ancient art documented use of cryptography in writing dates back, experts argue that cryptography appeared spontaneously sometime after writing was invented with applications ranging from diplomatic missives to war time battle plans. Cryptography not only protects data from theft or alteration but can also be used for user authentication, conceal the context of some message from all except the sender and recipient privacy or secrecy verify the correctness of a message to the recipient authentication, crypto analysis for transforming an intelligible message into an unintelligible one using a code.

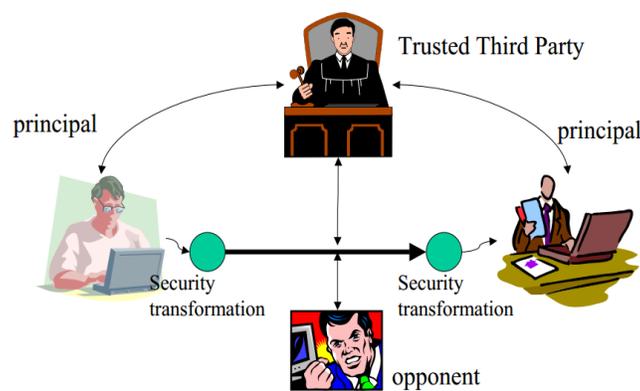


Figure 1 Method for secure data sending.

Steganography is time consuming to construct an arrangement of words or letters within an apparently innocuous text spells out the real message. The sequence of first letters of each word of the overall message spells out the real hidden message. Subset of the words of the overall message is used to convey the hidden message. Character marking is a selected letters or printed or typewritten text or overwritten in pencil marks are ordinarily not visible unless the paper is held to an angle to bright light. Invisible ink is a number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper and Pin punctures on selected letters are ordinarily not visible unless the paper is held in front of the light correction used between the lines typed with a black ribbon.

2. Related Work:

The purpose of Cryptography Steganography is a secret communication hides the contents of a secret message from an attacker whereas steganography even conceals the existence of the message. Breaking the system is different in cryptography the system is broken when the attacker can read the secret message breaking a steganography system has two stages.

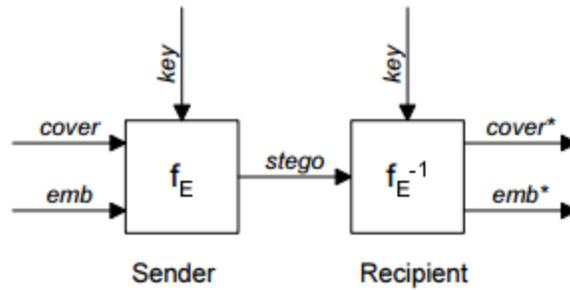


Figure 2 Concept of Steganography

Information hiding in Cambridge model embedding, input represents the untreated original data the one which will be embedded into cover by the function resulting data called stego contain the message operation extracts the embedded data and also produces an output cover, embedded data should be equal to emb and in most cases cover is the same as stego concealment systems cover is not much interest anyway. Model was not meant to be model for evaluating the security of steganography system by the participants for a beginning to put the ad-hoc knowledge of steganographic into a more abstract form for which purpose shown serves. Security of a steganographic system can see the acting entities the processing functions and their input and output describes the function and the knowledge capabilities of possible attackers.

3. Problem Definition:

Now a days people showing interest in online shopping, benefits the customers to save time and energy, E-marketing attracts the people but not protects the personal information. Bank details like debit or credit card numbers fraud personal information security of major concerns for customers and merchants to protect from this our analysis presents a technique with bit plane algorithm.

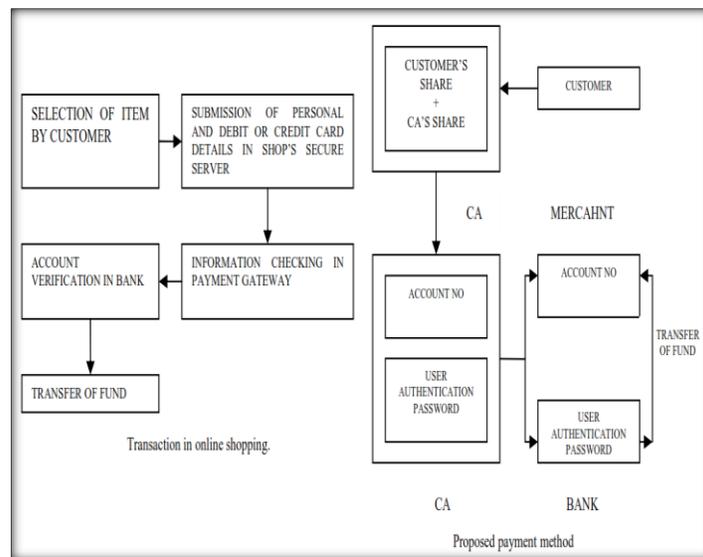


Figure 3 A Technique to avoid fraud on Online Shopping.

3.1. Bit Plane Slicing Segmentation Algorithm:

Instead of highlighting gray level images the contribution made to total image appearance by specific bits might be desired, suppose that each pixel in an image is represented by 8 bits. Imagine the image is composed of 8 1-bit planes ranging from bit plane 1-0 to bit plane 7 MSB, 8 bits plane 0 contains all lowest order bits in the bytes comprising the pixels in the image and plane 7 contains all high order bits.

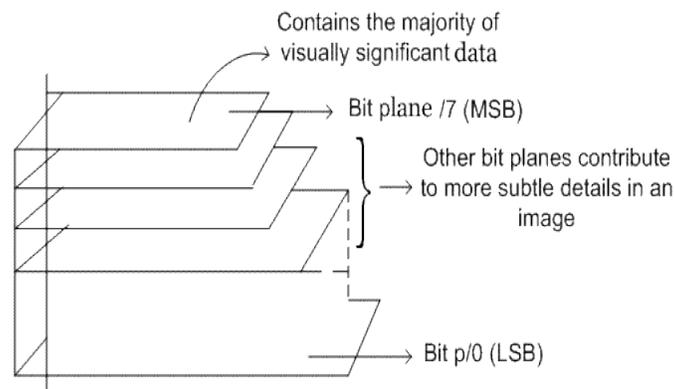


Figure 4 Approach of Bit Plane

Separating a digital image into its bit planes is useful for analyzing the relative importance played by each bit of the image implying determines the adequacy of numbers of bits used to quantize each pixel useful for image compression. In terms of bit plane extraction for 8-bit image it is seen that binary image for bit plane 7 is obtained by proceeding the input image with a thresholding gray-level transformation function that maps all levels between 0 and 127 to one level and maps all levels from 129 to 253 to another.

4.1. Method for Steganography: Steganography uses characteristics of English language such as inflexion fixed word order and use of periphrases for hiding data rather than using properties of a sentence gives flexibility and freedom from the point view of sentence construction but it increases computational complexity.

Representation of each letter in secret message by its equivalent ASCII code.

Conversion of ASCII code to equivalent 8 bit binary number

Division of 8 bit binary number into two 4 bit parts.

Choosing of suitable letters from corresponding to the 4 bit parts

Meaningful sentence construction by using letters obtained as the first letters of suitable words.

Encoding is not case sensitive.

Decoding is the process first letter in each word of cover message is taken and represented by corresponding 4 bit number.

4 bit binary numbers of combined to obtain 8 bit number

ASCII codes are obtained from 8 bit numbers

Finally secret message is recovered from ASCII codes.

4.2. Transaction Online Shopping: Online shopping consumer selects items from online shopping portal and then is directed to the payment page. Online merchant may have its own payment system or can take advantage of third party payment systems such as paypal pay online system web money and others. In the payment portal consumer submit credit or debit card details such as card number name on the card, expiry date of the card.

Customer unique authentication password in connection to the bank is hidden inside a cover text using the text based steganography method customer authentication information account no in connection with merchant is placed above the cover text in its original form. Now a snapshot of two texts is taken from the image two shares are generated using visual cryptography one share is kept by the customer and the other share is kept in the database of the certified authority.

4.3. Authorization Access: During shopping online after selection of desired item and adding it to the cart preferred payment system of the merchant directs the customer to the certified authority portal. The portal shopper submits its own share and merchant submits its own account details, authorization combines its own share with shoppers share and obtains the original image from authorization merchant account details cover text are sent to the bank where customer authentication password is recovered from the cover text. Finally authentication information is sent to the merchant by authorization access upon receiving customer authentication password bank matches it with its own database and after verifying legitimate customer transfers fund from the customer account to the submitted merchant account. After receiving the fund merchants payment system validates receipt of payment using customer authentication information.

5. Comparative Study:

Phishing is a criminal mechanism that employs both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. 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. In result to hide 4 letter word, 8 words are required excluding the words that are added to provide flexibility in sentence construction. So to hide a large message, this technique requires large no of words and creates a complexity in sentence construction. Disadvantage of this technique can be used in its advantage by applying it to online banking to create spam mail to hide one's banking information. In the proposed solution, information submitted by the customer to the online merchant is minimized by providing only minimum information that will only verify the payment made by the said customer from its bank account. This is achieved by the introduction of a central Certified Authority (CA) and combined application of Steganography and visual cryptography. The information received by the merchant can be in the form of account number related to the card used for shopping. The information will only validate receipt of payment from authentic customer.

- Proposed method minimizes customer information sent TRANSFER OF FUND to the online merchant.
- So in case of a breach in merchant's database, customer doesn't get affected. It also prevents unlawful use of customer information at merchant's side.
- Presence of a fourth party, CA, enhances customer's satisfaction and security further as number of parties are involved in the process.
- Usage of Steganography ensures that the CA does not know customer authentication password thus maintaining customer privacy.
- Cover text can be sent in the form of email from CA to bank to avoid rising suspicion.
- Since customer data is distributed over 3 parties, a breach in single database can easily be contented.

6. Conclusion:

Our work presents a technique for secure Online Shopping protects the personal information from fraud, potentially E-commerce is adopted by any password that tracks from any attack might effects the customer or merchant. This algorithm allows personal information major security concerns debit or credit details when card is not present. In addition, limited information only that is necessary for fund transfer during online shopping, Bit Plane algorithms for the online shopping that protects from fraud could achieve quality effectiveness of our solution.

References

2. B. Pfitzmann, "Information Hiding Terminology". In R. Anderson, Information Hiding: first international workshop, Proceedings (Lecture notes in computer science; Vol. 1147), Berlin: Springer, 1996.
3. J. Zöllner, H. Federrath, A. Pfitzmann, A. Westfeld, G. Wicke, G. Wolf, "Über die Modellierung steganographischer Systeme". In G. Müller, K. Rannenberg, M. Reitenspieß, H. Stiegler, Verlässliche IT-Systeme. Zwischen Key-Escrow und elektronischem Geld, Friedr. Vieweg & Sohn Verlagsgesellschaft mbH, Braunschweig/Wiesbaden, 1997, pp. 211-223.
4. H. Klimant, R. Piotraschke, "Informationstheoretische Bewertung steganographischer Konzellationssysteme". In G. Müller, K. Rannenberg, M. Reitenspieß, H. Stiegler: Verlässliche IT-Systeme. Zwischen Key-Escrow und elektronischem Geld, Friedr. Vieweg & Sohn Verlagsgesellschaft mbH, Braunschweig/Wiesbaden, 1997, pp. 225-232.
5. R. Anderson, F. Petitcolas, "On the limits of steganography". To be published in IEEE Journal on Selected Areas in Communications, Special Issue on copyright and privacy protection. Available at: <http://www.cl.cam.ac.uk/ftp/users/rja14/steganjsac2.ps.gz>



Sana Shiva pursuing M.Tech CSE from Brilliant Institute of Engineering & Technology B.Tech CSE from Aryabhata Institute of Technology & Science. His research areas include Computer Networks, Security, Social Networks.



A.Hari Teja B.Tech CSE from Gokula Krishna College of Engineering M.Tech Software Engineering from VTU Bangalore M.Tech A.I from JNTUA. He is having 8 years of Experience in Academic currently working as Assoc Prof at Brilliant Institute of Engg & Tech guided many UG & PG students. His research areas include Machine learning, Neural Networks, Text Processing, Knowledge Representation & Reasoning.