Design Securing Online Payment Transactions Using Stegblock Through Network Layers.pdf

by Eka Ardhianto

Submission date: 30-Nov-2020 07:01PM (UTC+0700)
Submission ID: 1460162384
File name: Design Securing Online Payment Transactions Using Stegblock Through Network Layers.pdf (1.07M)
Word count: 3373
Character count: 17813

Design Securing Online Payment Transactions Using Stegblock Through Network Layers

Design Securing Online Payment Transactions Using Stegblock Through Network Layers

E Ardhianto[1*], A Trisetyarso[2], W Suparta[3], B S Abbas[4] and C H Kang[5]
[1,2,4,5]Computer Science Departement, BINUS Graduate Program – Doctor of Computer Science, Bina Nusantara University, Jakarta, Indonesia.
[1]Faculty of Information Technology, Universitas Stikubank, Semarang, Indonesia.
[3]Departement of Informatics, Universitas Pembangunan Jaya, South Tangerang, Banten, Indonesia

Email : *ekaardhianto@edu.unisbank.ac.id

Abstract. The aim of this work is designing a safe online payment activities scheme using steganography techniques with stegblock concept. These works are implemented at the computers network layers. The stegblock will convert the transactions data which sent among network into other data's form, it means the data such as ID Number, Account Number, Passwords and others are converted with other data called cover. Finally, the system sends the cover without the real data, it just represented data and able to read by the receiver. The result shows that this design provides data security, undetectability, and integrity for payment transactions using networks.

1. Introduction

Online transaction data such as identity numbers, passwords, verification codes, account numbers are data that need to be protected. This especially, if the payment transactions of data transfer made through an open network. Crime and fraud can be happened during the online shopping transaction process. Sometimes the transaction process also involves a third party besides the seller and buyer. This will also be issued an assessment of the buyer's trust in the security of the data, which at the time the transaction is carried out by the line. So, a special mechanism is needed to secure data sent through the online network during the transaction process. In this case, buyer and seller have a role as sender or receiver of datas transaction.

Data security techniques are generally known as cryptography. Cryptography secures data by changing data into other forms that are meaningless. Steganography technique is different from cryptography, which is securing data by utilizing another data called a cover which serves to hide the original data inside it.

Safeguarding data by issuing a Certificate Authority (CA) by applying Dual Enchipering Mechanism (DEM), it combines both steganography and cryptographic techniques. Cryptography techniques are used to secure data, while steganography techniques are used to hide data [1]. Other research conducted a survey of online transaction data security, this survey concluded that security can be created by involving human biometric attributes such as fingerprints, face, and iris. Which is then combined with a PIN and One Time Password (OTP) in conducting online transactions [2].

Online transactions certainly use computer devices connected to the communication network. This network will connect devices belonging to buyers, sellers, and devices belonging to third parties. Computers have network devices known as network layers. The networking steganography technique has so far progressed. Some development in network steganography is done in the physical layer and transport layer by manipulating timing and delay [3]. Another paper also performs network steganographic techniques by observing and identifying packet flow in IPv4 [4].

Some of the development of Steganography in the network transport layer include securing communication by applying steganography and cryptography [5], a paper proposes by implementing the RSA encryption algorithm and continuing to change the ciphertext into ASCII code, hexadecimal numbers until binarization and then broken up to 20 bits per packet and then sent over a computer network [6]. Another method that has been proposed is to reduce the size of packets transmitted over a computer network, this will avoid packet congestion in the communication path [7]. The process of steganography networking also uses multi-level security techniques that involve the use of secret matrices, secret keys and hidden signatures [8], a hidden signature was also developed using the timestamp as an additional attribute [9]. Development with the permutation process with tables has also been proposed [10].

The development of data security is also carried out on the mechanism of online transactions. A framework is proposed for securing transaction data in the cloud, called CSTAE-PSTO (conditional source trust attribute encryption with particle swarm-based transaction optimization) framework for transaction security in cloud data. This framework efficiently generates encryption and decryption processes using the bilinear mapping transformation function based on a specific id number [11]. Safekeeping of transaction data with steganography and cryptography was made by entering messages in to cover image using Discrete Wavelet Transformation (DWT) technique which is then converted to binary and stored at the merchant and user database, so that when making a transaction only by making a combination of both [12]. Other development uses the value comparison of certificate authentication (CA) and generate One Time Password (OTP) and upgrading communications using 2048bit Socket Secure Layer [13]. A Cyclic Shift Transposition Algorithm (CSTA) is proposed to secure data transactions by involving the use of the QR Code and Hash Timestamp to increase data confidentiality [14]. The addition of a layer of security to prevent fraud is also proposed, by analyzing web browser cookies and geographical location by recording coordinates to generates OTP [15]. Identification of e-money transactions is also proposed with three layers of security by merging pin numbers, usernames and biometrics, which then uses confirmation codes and machine coordinate positions to guarantee the authenticity of users [16]. Verification via the MAC address of the computer to register the OTP sent to the mobile device is also proposed [17]. A modified blowfish algorithm is also used [18]. The Secure Online Transaction Algorithm (SOTA) algorithm was also developed using random codes and hash functions from transaction data [19].

Stegblock is a concept for hiding data that is communicated [20]. The use of stegblock is implemented in steganography networking. This uses a specified cover object as a secret data carrier that will be transmitted. This stegblock concept is designed perfectly to hide data because the cover object that is sent will not experience distortion when received.

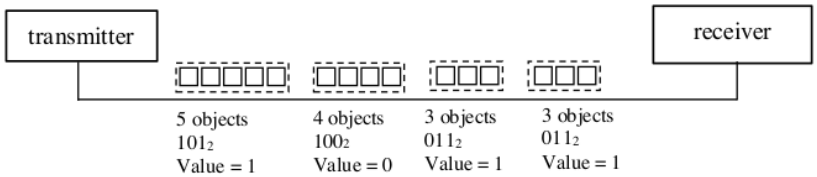

Figure. 1. Image of Stegblock Concept, adopted from [20].

Stegblock works in the network layer. It starts with defining an object with an n identifier and specifying k as key. The selected objects are merged into a sequence called blocks. A block is determined

by its minimum length by counting the key k as part of the block. The beginning and end of the block are given a marker. Each block will contain a number of objects, the value of a block is the last bit of the number of objects in the block after converted in binary form. For example, if the block contains 5 objects it implies 1 because the binary shape of 5 is 101_2. If it contains 4 objects it will imply 0, because 100_2 is a binary form of 4, and if it is 3 it will also imply 1 (**Fig. 1**). The value of the block indicates as the message sent, and merged by a receiver.

This paper discusses a safer online payment transaction design made by utilizing networking steganography techniques. This work uses the stegblock concept by adding several processes to create a stream block segment (SBS).

2. Method

2.1. Design Stegblock in Securing Online Payment Transaction

Based on previous research, the data transaction is still passed through the network line even though security processes have been carried out. With stegblock, the data sent are only covered which represents the original data. In this section, we will discuss the design of online payment transaction data security using the stegblock concepts by adding several processes to support data security as shown in Figure 2.

The flow of Design Securing Online Payment Transaction (**fig. 2**) can be explained as follows. Secret data is the original data that will be used to make payment transactions. Secret data can be consist of account numbers, credit card numbers, payment amounts and others that are confidential. Cover data is data that is used as a cover in the steganography process.

The next step is calculating the length and number of blocks needed to define the size of the segment. In this step, it is required data secret and data cover as input. The result of this process is the number and length of blocks needed for the steganography process.

The process is continued by taking and identifying the size of the payloads which flow on the sender devices's network and proceed with the calculation of the value of a payload save the number. Payload save number means that the payload size that will be used to create a block will be similar to other segments that circulating on the network, this will reduce suspicion. If the size of this segment is too small or too large, it might raise suspicion.

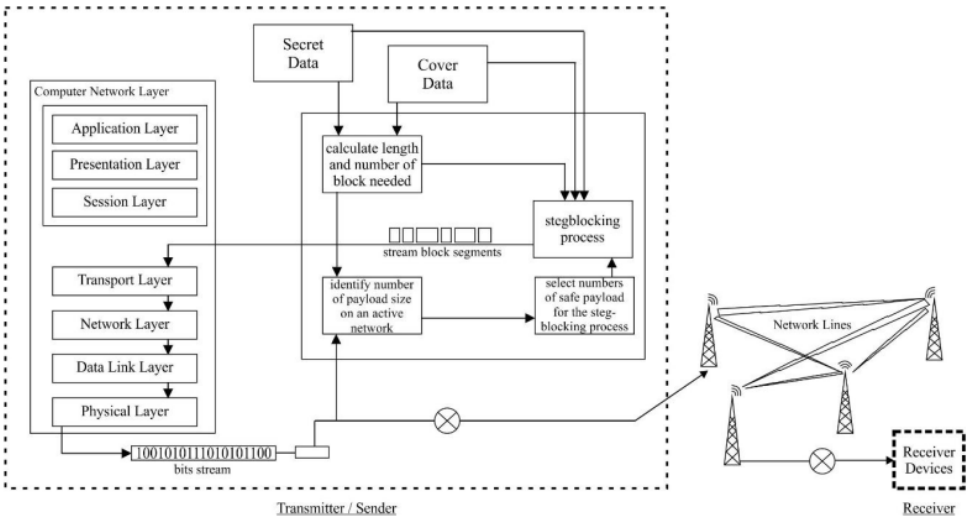

Figure. 2. Design of Securing Online Payment Transaction using Stegblock Concept

The results of the calculation of segment size, segment length and number of segments will processed with secret data and data cover in the steganography process using stegblock concept. This output

process is block flow that represents the value of the data secret which in this paper is called the stream block segment (SBS). The SBS will forward into the transport layer on the network for the encapsulation process and sent it through the network line. The receiver receives and reads the message by looking at the value of each segment block and converted to secret data that can be read properly.

3. Results and Discussions

3.1. Features of Design

There are several features of Design Securing Online Payment Transaction that are provided in terms of data security, Privacy, Undetectbility, and Integrity.

The privacy aspect is the confidentiality aspect of the data, in this design the confidentiality of the data is guaranteed by the process of concealing data secrets using data cover. In this case, the data secret will be replaced by the data cover during the trip. Another secrecy is the stegblock process, in this process, the cover data which sent has been split into several block segments which are sent through the transport layers. From the sent segment, the outstanding value is not the original value of the data secret but is the value of the data cover. This is if there is data theft by an unauthorized person, only data cover will appear.

The second aspect is the undetectability. Cover data which sent over the network will be difficult to detect. This is because there is a payload safe number calculation. This aspect is also supported by the steganography process which is hiding secret data by using data cover.

Unity of confidential data which known as integrity, is also important. In the design, the integrity of the data received will be put back together through the network layers device by detecting squence number of message's packets. The sequence number produced by the transport layer will identify the sequence of messages transmitted on the receiving device

3.2. Posibility of Attacking

The scenario of designing the Securing Online Payment Transaction is expected to be able to withstand several possible attacks. The first attack was the theft of data in network transmission. This will keep data secrets safe because the data that is in the network is not data secrets but data covers. So if the data in the network is known by unauthorized persons, what is seen is not the actual data secret.

The second attack is dropping or delaying or withholding some of the data transmitted. If this happens there are two things that will anticipate it. The first is that the nature of the transport layer is to reorder sequences if there is an incomplete packet sequence the transport layer will ask the sender to resend the packet data. The second is that if the time limit of the messages has expired, it means the time to live the parts of the frame, then the application can append a function that produces information for the recipient that there is some data incomplete, so the recipient will ask the sender to repeat the process.

Another possibility of attacking is that the time to live for all frames ends. This will make data sent has failed status. This is not a serious problem because the recipient also will not accept transmitted data transmissions, and the sender will receive an information that data was unsuccessful to be transmitted and it can be retransmitted.

3.3. Zero MSE

Based on Figure 2, both sender and receiver will have data cover which transmited on line. Quality of data cover distortion can be measured with Mean Square Error (MSE). MSE of data cover calculates from average of squares data values of input and output data cover. Peak Signal to Noise Ratio (PSNR) is a quantitative measure to identificate quality of data cover based on differences of values between data cover and it's result [21]. MSE and PSNR are calculated using equations as follows.

$$\mathrm{MSE} = \frac{1}{MN} \sum_{J=1}^{M} \sum_{k=1}^{N} \left(x_{j,k} - x'_{j,k}\right)^2 \quad (1)$$

N and M refer as size or dimension of data cover, j and k are coordinates of data's cover value, x is input value and x' is output value.

$$\text{PSNR} = 10 \log_{10} \frac{C^2}{MSE} \quad (2)$$

C refers to maximum value of data cover.

Value of PSNR and MSE are inversely proportional, this implies if lower MSE value then higher PSNR value. So, it means that higher PSNR makes better output, cause it has fewer error [22].

In this case, sender will send data cover to receiver. The data cover does not have any changes, it only splitted into several blocks which represent the messages. So, the receiver will have the same data cover. The MSE calculations will use the value of every values of both data cover, which sender and receiver have. If $x_{j,k}$ filled with value of data cover in sender side and $x'_{j,k}$ with data cover in receiver side, then *M* and *N* filled with dimension of data cover , it resulted that MSE's value is 0. This is caused by $x_{j,k}$ and $x'_{j,k}$ have same values, then it's result devided by *M* and *N* it's also resulted 0 value. So, MSE's value is 0. With 0 value of MSE, it means the data cover will expected has not differences between before and after it transmited.

4. Conclusion

This paper provides the design of Securing Online Payment Transactions using the stegblock concept. It shows how to secure data sent over a computer network using the stegblock concept. This design provides benefits for payment transaction that are carried out online. This model uses two safety factors, namely using stegblock as a steganographic concept and using payload safe number calculation. Based on the discussion and possible attacks, this design provides security for data and online payment transaction's processing, even more the values of PSNR and MSE's are predicted have good values. Improving the design and fill in the gaps of all possible attacks on data to be secured and sent through the network layer of the computer still need to be considered as future works.

References

[1] Amar C, Sultanhusen S, Vashista G, D S V and Raza N 2017 A Review - Transaction Security Using Steganography and Visual Cryptography *International Journal of Scientific Research in Sci Engineering and Technology* p. 597-600.

[2] Priya H M and Lalithamani N 2017 A Survey for Securing Online Payment Transaction Using Biometrics Authentication *Advances in Intelligent Systems and Computing* p. 81-91.

[3] Seo J O, Manoharan S and Mahanti A 2016 A Discussion and Review of Network Steganography in *2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing*.

[4] Kheddar H and Bouzid M 2015 Implementation of Steganographic Method Based in IPv4 Identification Field over NS-3 *International Journal of Engineering Research and Applications* **5(3)** p. 44-48.

[5] Dalal S and Devi S 2017 Security Framework against Denial of Service Attacks in Wireless Mesh Network *Global Journal of Pure and Applied Mathematics* **13(2)** p. 829-837.

[6] Bobade D and Goudar R 2015 Secure Data Communication Using Protocol Steganography in IPv6 in *IEEE 2015 International Conference on Computing Communication Control and Automaton*.

[7] Gulia p and Reena 2017 A Novel Technique of Security Improvement in Ad-hoc Network by using FTP *International Journal of Applied Engineering Research* **12(17)** p. 6658-6662.

[8] Venkadesh P, Dhas J P M and Divya S V 2015 Techniques to enhance security in SCTP for multi-homed networks in *IEEE : 2015 Global Conference on Communication Technologies (GCCT)*.

[9] Ruban I, Chuiko N L, Mukhin V, Kornaga Y, Grishko I and Smirnov A 2018 The Method of Hidden Terminal Transmission of Network Attack Signatures *International Journal Computer Network and Information Security* **4** p. 1-9.

[10] Peng F X, Jing S H and Rong G H 2017 A New Network Steganographic Method Based in The Transverse Multi-Protocol Collaboration *Journal of Information Hiding and Multimedia Signal Processing* **8(2)** p. 445-459.

[11] Brindha T and Shaji R S 2016 A Secure Transaction of Cloud Data using Conditional Source Trust Attributes Encryption Mechanism *Soft Computing* p. 1013-1022.

[12] Devi M D A and Kumar K B S 2017 A Novel Image Steganography Technique for Secured Online Transaction Using DWT and Visual Cryptography *IOP Conf. Series: Materials Science and Engineering*.

[13] Ruman K and Phaneendra H D2015 Implementation of Methods for Transaction in Secure Online Banking *International Journal of technical Research and Applications* p. 41-43.

[14] Neela K L and Kavitha V 2018 Enhancement of Data Confidentiality and Secure Data Transaction in Cloud Storage Environment *Cluster Computing* p. 115-124.

[15] Kulat A, Kulkarni R, Bhagwat N, Desai K and Kulkarni P 2016 Prevention of Online Transaction Frauds Using OTP Generation Based on Dual Layer Security Mechanism *International Research Journal of Engineering and Technology* p.1058-1060.

[16] Islam M S 2015 An Algorithm for Electronic Money Transaction Security (three Layer Security) : A New Approach *International Journal of Security and Its Applications* p. 203-214.

[17] Basharat A, Naz M and Afzal K 2016 Prevention of Online Transaction Using MAC Address of the Machine, OTP Two Layer Model to Identify Legitimate User *Journal of Culture, Society and Development* p. 30-32.

[18] Iqbal S and Yadav R L 2018 A Secure File Transfer Using the Concept of Dynamic Random Key, Transaction Id and Validation Key with Symmetric Key Encryption Algorithm in *Proceedings of First International Conference on Smart System, Innovations and Computing, Smart Innovation, Systems and Technologies*, (Singapore).

[19] Gualdoni J, Kurtz A, Myzyri I, Wheeler M and Rizvi S 2017 Secure Online Transaction Algorithm: Securing Online Transaction Using Two-Factor Authentication in *Complex Adaptive Systems Conference with Theme: Engineering Cyber Physical Systems*, (Chicago).

[20] Fraczek W and Szczypiorski K 2016 Perfect Undetectability of Network Steganography *Security and Communication Networks* **9(15)** p. 2998-3010.

[21] D. Shehzad and T. Dag 2019 LSB Image Steganography Based on Blocks Matrix Determinant Method *Transactions on Internet and Information Systems* **13(7)** p. 3778-3793.

[22] A. Sathyan, M. Thirugnanam and S. Hazra 2016 A Novel RGB Based Steganography Using Prime Component Alteration Technique *IIOAB Journal* **7(5)** p. 58-73.

Design Securing Online Payment Transactions Using Stegblock Through Network Layers.pdf

ORIGINALITY REPORT

8%	7%	7%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to University of Greenwich Student Paper	3%
2	mafiadoc.com Internet Source	2%
3	eprints.umsida.ac.id Internet Source	1%
4	Thomas Brindha, Ramaswamy Swarnammal Shaji. "A secure transaction of cloud data using conditional source trust attributes encryption mechanism", Soft Computing, 2016 Publication	1%
5	www.science.gov Internet Source	<1%
6	"Proceedings of First International Conference on Smart System, Innovations and Computing", Springer Science and Business Media LLC, 2018 Publication	<1%

7	Andik Setyono, De Rosal Ignatius Moses Setiadi. "Imperceptible Improvement of Secure Image Steganography based on Wavelet Transform and OTP Encryption using PN Generator", Journal of Physics: Conference Series, 2019 Publication	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		