IJIRR

International Journal of Information Research and Review
Vol. 03, Issue, 03, pp. 2010-2013 March, 2016

Research Article

A SECURE MOBILE COMMERCE USING RANDOM LEAST SIGNIFICANT BIT STEGANOGRAPHY ALGORITHM

***[1]Sridhar, K., [2]Dr. Suresh Babu, D. and [3]Dr. Venugoapl, T.**

[1]Research Scholar, Department of CSE, JNTUH, Telangana, India
[2]Supervisor, HOD CSE Department, KGC Warangal, Telangana, India
[3]Co-Supervisor, Associate Professor, JNTUCEJ, Sulthanapoor,Telangana, India

ARTICLE INFO

Article History:

Received 18th, December 2015
Received in revised form
28th, January 2016
Accepted 17th, February 2016
Published online 31st, March 2016

Keywords:

Cryptogarphy, LSB,
M-Business Steganogaphy.

ABSTRACT

M-business is one of the major branches of e-business. The maintenance money industry is among the main divisions in receiving and using the Internet and portable innovation on shopper markets. Portable managing an account is a subset of electronic managing an account which under lies not just the determinants of the managing an account business additionally the extraordinary states of portable business. The advancement of electronic managing an account and portable managing an account administrations by means of different channels has made it conceivable to make new sorts of included quality for clients. Be that as it may, in resentment of their preferences, both are confronting a few difficulties as well. One of these difficulties is the issue of security of these frameworks. This paper presents security of these frameworks utilizing Arbitrary LSB steganography and cryptography system. The proposed strategy is more protected and secure as opposed to utilizing either steganography or cryptographic strategy. This paper shows secure and imperceptible correspondence in M-keeping money and in addition e-saving money

INTRODUCTION

M-business is one of the principle branches of e-business. The keeping money industry is among the main divisions in receiving and using the Internet and portable innovation on shopper markets. Portable managing an account is a subset of electronic managing an account which under lies not just the determinants of the managing an account business additionally the extraordinary states of portable business. The advancement of electronic managing an account and portable managing an account administrations by means of different channels has made it conceivable to make new sorts of included quality for clients. Be that as it may, in resentment of their preferences, both are confronting a few difficulties as well. One of these difficulties is the issue of security of these frameworks. This paper presents security of these frameworks utilizing Arbitrary LSB steganography and cryptography system. The proposed strategy is more protected and secure as opposed to utilizing either steganography or cryptographic strategy. This paper shows secure and imperceptible correspondence in M-keeping money and in addition e-saving money. In this paper rather than direct sending data, it is scrambled first utilizing encryption calculation and after that this scrambled data is handled to stow away into a picture utilizing a secret word so that stego-picture contains shrouded message which is not in plaintext structure. Another essential point is that scrambled data is covered up into a picture utilizing "Arbitrary LSB Steganography" that is implanting information in non consecutive LSB insertion design with the goal that it is garbled and hard to recognize. The stego-picture is put on a site then the URL of the site is sent to the client. In the wake of accepting the URL, the client downloads the photo by an extraordinary project. The client can separate data from the photo just if the secret key entered is right. This data will be in encoded structure client will decode it utilizing the unscrambling calculation so that client will get obliged data. The proposed plan has been executed utilizing J2EE dialect for e-saving money and J2ME dialect for m-managing an account. Our execution underpins all java empowered mobiles for m-managing an account application.

Corresponding author: Sridhar, K.
Research Scholar, Department of CSE, JNTUH, Telangana, India.

Algorithm

Ordinarily in e-managing an account and m-keeping money client demands such as credit equalization of the record. Data is sent specifically after the client demand. While sending data straightforwardly it is conceivable that programmers may get to and unveil the client's data.

Encryption Algorithm

The encryption calculation that we utilized is the AES Rijndael calculation . AES Rijndael is an iterated piece figure, implying

that the starting information square and figure key experience various change cycles before creating the yield. The calculation can work over a variable-length piece utilizing variable-length keys; a 128-, 192-, or 256-bit key can be utilized to scramble information obstructs that are 128, 192, or 256 bits in length, and each of the nine mixes of key and square lengths are conceivable. The calculation is composed so that piece length and/or key length can without much of a stretch be reached out in products of 32 bits, and the framework is particularly intended for productive execution in equipment or programming on a scope of processors.

AES Rijndael is a substitution-straight change system with 10, 12 or 14 rounds, contingent upon the key size. An information piece to be encoded by AES is part into a variety of bytes, and every encryption operation is byte-arranged. AES's round capacity comprises of four layers. In the first layer, an 8x8 S-box is connected to every byte. The second and third layers are straight blending layers, in which the columns of the cluster are moved, and the sections are blended. In the fourth layer, subkey bytes are XORed into every byte of the cluster. In the last round, the section blending is precluded. The AES Rijandael execution was taken from the Legion of the Bouncy Manor cryptographic bundle which gives a Java execution for the calculation.

In our application we utilized a square size of 16 bytes prepared with 128-bit keys: this ended up being the best blend for operation on J2ME gadgets because of the velocity.

Fig. II. 1 BMP *picture as Cover-picture*

Fig. II. II BMP picture as Stego-picture

What's more, memory restrictions of such gadgets? The customer and the server utilize two 128-bit keys, one for every course of information travel. That is, one key is utilized to scramble the information in the customer and decode it in the server, and the other is utilized to scramble the information in the server and decode it in the customer. Towards the beginning of each customer session, the server arbitrarily creates this pair of keys and stores them in the customer's particular passage in the database. The server then encodes these session keys utilizing the customer's 64-bit pin code cushioned to a 64-bit shared mystery known not customer and the server.

LSB Stenography

This technique shrouds data at all noteworthy bits of pixels. In this technique every byte of data is covered up in two pixels. For concealing data a byte is isolated into a eight bits. By utilizing secret key two pixels are chosen in which a byte of data is covered up. A calculation in [1] is used to choose pixels to conceal information.

In this calculation picture is divided into n piece of m pixels. A piece is chosen by and the data is covered up in a vacant pixel of this square. The calculation for selecting a piece and an unfilled pixel in that obstruct as takes after:

In the event that the chose piece begins with the pixel number x and has m pixels then the quantity of last pixel is x+m-1. This calculation utilizes a variety of size m+1 for recalling void pixels of current piece. This cluster contains the quantity of pixels having no information. The last cell of the cluster is the aggregate vacant pixels in the present piece. As indicated by the secret word, a void pixel is chosen and the last discharge pixel number is duplicated to this cluster cell. After this operation the aggregate number of void pixels on the piece diminishes by one. This strategy is additionally utilized for selecting a piece to shroud the data in itself. Subsequent to selecting the pixels we conceal a byte inside of them. Each pixel has three hues (RGB), and the data is put away in the LSB of these hues.

Advantages

1. This method is compatible with many types of mobile phone.
2. In this method before steganography in the picture, encrypted information is encoded by a password therefore if person manages to extract information from the picture he will not be able to decode it without having the password.
3. In this method the information is never placed on the internet. Thus, the possibility of disclosure of information is very low.
4. In this method use of combination of steganography and cryptography provides strong secure and invisible communication.
5. The Random LSB steganography algorithm advantages are:
a. Message is embedded in non sequential LSB insertion pattern so it is difficult to detect LSBs in which message is embedded.
b. Because the password is used, it is difficult to detect the information hidden in the image.
c. The decoding program uses a few kilobytes of memory. Also the program is fast enough.
6. For each access to bank service we are using security code which is known to that particular user.

Implementation

The application we outlined and executed gives a model answer for securing delicate information. This area presents a brief

dialog of the outline beginning with the customer environment and proceeding onward to the server environment. In this paper we are depicting execution of m-managing an account administration.

The Customer Environment

On the customer side we utilized the J2ME remote toolbox 1.0.4 gave by Sun. The remote toolbox is an arrangement of instruments that furnish J2ME engineers with the imitating situations, documentation, and samples to create MIDP-agreeable applications. Engineers are in this manner ready to check the substantial operation of their applications before conveying them on genuine physical gadgets. The MIDP application is bundled inside a Java chronicle (Jug) document, which contains the application class and asset records. This Jug document is really downloaded to the physical gadget (cell telephone) along with the Java application descriptor record.
In the customer environment client sends solicitation, gets location of site on which picture is spared, downloads picture, extricates data from picture and decodes data to get obliged results. After these operation client can do saving money administrations like record equalization, exchange, mini statement, check and so on. Amid inside and outside exchange client needs to give secret word which client utilized at the time of extricating data from a picture. On the off chance that watchword is wrong then exchanges get fizzled.

The Server Environment

To profit by an immaculate Java arrangement, we actualized the server-side application as per the J2EE details. Servlet classes are bundled in a web document (WAR) record and conveyed on the J2EE application server. We utilized the J2EE reference execution server adaptation 1.3.1 gave by Sun. The database server we utilized is the Microsoft SQL Server. The Java Servlets speak with the database utilizing the surely understood Java database integration (JDBC) Programming interface and the new javax.sql bundle. A portion of the administrations tended to by the javax.sql bundle are association pooling, conveyed exchanges and information source recovery utilizing intelligent names. Rather than stacking the particular JDBC driver every time we need to interface with the database, we utilized the Java naming and index interface (JNDI) to recover the information source utilizing its consistent name from a JNDI-protestation index administration on the J2EE server. In the server environment there is verification Servlet to verify customer, administration Servlet which gives administrations asked for by customer like record parity, exchange, mini statement, check and so on. This environment likewise contains encryption system and lsb encoding project. In our technique rather than direct sending data in plaintext structure we are encoding this data utilizing "Propelled Encryption Standard" calculation and after that encoded data is covered up into the photo by utilizing secret key and "Irregular LSB Steganography calculation". This stego-picture is set in another site and location of that site is sent to client. Client downloads the photo from site. Client separates data from picture by utilizing secret key then client gets data in encoded structure. Client decodes data with the goal that he gets result. These systems demonstration as takes after;

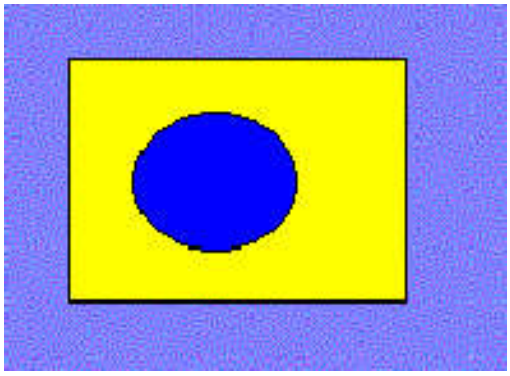

Fig. IV. I. ***GIF picture as Cover-picture***

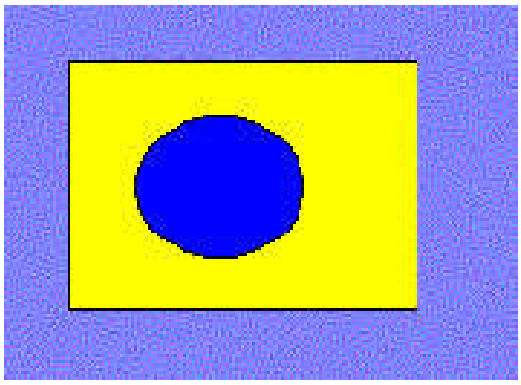

Fig. IV. II. ***GIF picture as Stego-picture***

Conclusion

In this paper we have shown that security of e-commerce and m-commerce has been improved using random LSB steganography and cryptography method together instead of using either steganography or cryptography. Steganography algorithm can be changed based on the requirements of concerned m-banking system. Also, we can choose the encryption algorithm depending upon the processing timer acquired to encrypt the information. This method can be used on all types of java enabled mobile devices

Acknowledgment

We would like to thank to all the faculty members of department of computer science and my friends for their good wishes, their helping hand and constructive criticism which led the successful completion of this paper. We thank all those who directly and indirectly helped us in this regard.

REFERENCES

Anurag Kumar Jain *et al*. 2012. Addressing Security and Privacy Risks Mobile applications. IEEE Computer society.

ArunKumar Gangula *et al*. 2013. Survey on Mobile Computing Security. IEEE Computer Society.

Ashok K Talukder *et al*. 2005. Mobile Computing. TaTa McGraw Hill Education, January.

Bernaard menezes, 2015. Network security and cryptography. CENGAGE Learning,second edition.

Boyd, C. *et al*. 2001. Curve Based Password Authenticated Key Exchange Protocols. LNCS Vol. 2119, pp. 487-501.

Boyd, C. *et al*. 2001. Elliptic Curve Based Password Authenticated Key Exchange Protocols. LNCS Vol. 2119, pp. 487-501.

CUI Jian-qi *et al*. 2007. New secure mobile Electronic commerce solution based on WA. Application Research of Computers Vol.24.

Dharma prakash agrawal *et al*. 2015. Introduction to Wireless and Mobile Systems. Third Edition, Cengage Learning USA

Feng Tian *et al*. 2009. Application and Research of Mobile E-commerce security based on WPKI. IEEE International Conference on Information Assurance and Security.

Fourati *et al*. A. 2002. A SET Based Approach to Secure the Payment inMobile Commerce. In Proceedings of 27th Annual IEEE Conference on Local Computer Networks (LCN'02), Tampa, Florida

Yee, B.S. 1994. Using Secure Coprocessor, PhD thesis, Carnegie Mellon University.

****