ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

A Survey on Techniques of Data Hiding Using Steganography and Visual Cryptography

Mrunali V. Kale[1], Shreya B. Pardeshi[2], Aniket S. Pardeshi[3], Prof. Amrut V. Kanade[4]

Student, Dept. of Comp, Pune, India

Student, Dept. of Comp, Pune, India

Student, Dept. of Comp, Pune, India

Assistant Professor, Dept. of Comp, Pune, India

ABSTRACT: In recent time E-Commerce is rapidly growth in E-Market specially for online shopping system. With ever Increasing popularity of online shopping, Debit or Credit card wrongful and personal private information security are major concerns for customers, merchants and banks. Personal information and there misuse of that information for making purchase and bank accounts or arranging credit cards. The main motive of the proposed system prescribed in this paper is to handle applications that requires a high level of security, like E-Commerce applications, core banking and internet banking. This can be done by using combination of two methods: Text based Steganography and Visual Cryptography for safe online shopping and consumer satisfaction. This is achieved by the introduction of Central Certified Authority (CA) and combined application of Steganography, Visual Cryptography for this purpose.

KEYWORDS: Data Hiding, Steganography, Visual Cryptography

I. INTRODUCTION

A large number of countries such as India, China and Pakistan that have some problems to become overcome in regard to credit card security such as in 2012 cardholders information was misused for average of 48 days as a result identity theft. In Online shopping the issue of purchase order through with help of electronic purchase request ,filling of credit or debit card information. Identity theft or phishing are the dangers in E-Commerce's. Identity theft is the stealing of someone's identity in the form of personal information and miss use. A new method is proposed, that uses text based steganography and visual cryptography, which limited formation sharing between customer and online merchant but enable successful fund transfer and preventing misuse of customer information.

Steganography is art of sending hidden or invisible messages. The name is taken "Steganography" it is Greek world στεγανό-ς,γραυ-ειν meaning "covered writing" .The sending secret messages and attempts to cover the messages by hiding them by making them look like something else have been made .In Short Stenographic is information can be hidden in almost anything, While much of modern steganography focuses on images, audio and other digital data, there is also a wealth of text sources in which information can be hidden. That are the various ways to hide information in text, there is a specific set of techniques which are uses. Certification Authority (CA) which has provides Key Infrastructure for STEGANOGRAPHY TECHNIQUES and Transform techniques are used. The Least significant bit (LSB) algorithm having a simple insertion technique to embedding information in image file. The simplest steganography techniques embed the bits of message directly into least significant deterministic sequence having bit plane of the cover-image in it. Because the amplitude of the change is small, So that modulating the least significant bit does not result in human perceptible difference. In this paper, the embedding capacity can be increased by using two or more least significant bits. At the same time, not only the risk of making the embedded messages statistically noticeable increase but also the image fidelity degrades. Therefore a variable size LSB embedding schema is presented, in which the number of LSBs used for message extracting depends on the local characteristics of the pixel. LSB-based method is easy to implement and high message pay-load is the main advantage.

LSB hides the message in such way that the humans do not perceive it, is it still possible for the opponent to retrieve the message due to the simplicity of the technique. Therefore, malicious people can be easily try to extract the message from the beginning of the image if they are suspicious that there exists only secret information that was

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

embedded in the image. Therefore, a system named Secure Information Hiding System (SIHS) is propose to improve the LSB scheme. It overcomes the problem of sequencing-mapping by embedding the massage into a set of random pixels, which are scattered on the cover-image. Usually restricted to 24 bits and gray scale image, hide information by marking an image, in a manner similar to paper watermarks the Masking and filtering techniques are used. The technique perform analysis of the image, thus embed the data information in significant areas so that the hidden message is more integral to cover image than just hides it in the noise level. Transform techniques embed the message by modulating coefficient in a transform domain, such as the Wavelet Transform or Discrete Fourier Transform. These techniques hide messages in specific areas of the cover Images, which all makes them more robust to attacks. Transformations can be applied over the entire image, to block throughout the image, or other variant. Cryptography is securely related to the disciplines of cryptology and cryptanalysis.

Cryptography includes methods such as microdots and merging words with images, and other ways to hidden information in storage or transit. However, in today's computer-centric world and cryptography is most often associated with scrambling plaintext (sometimes it referred to as clear text) into cipher text (that process called encryption), then back again(known as decryption). Cryptographers means Individual who practice this field. the information cannot be understood by anyone for whom it was unintended the information cannot be altered in storage or transit between sender and receiver without the alteration being detected the creator/sender of the information cannot deny at a remaining stage his or her intentions in the creation or transmission of the information the sender and receiver can confirm each other's identity and the origin/destination of the information.

Cryptography has changed into a battleground of some of the world's best mathematicians and computer scientists. The ability to securely store and transfer sensitive data or information has proved a critical factors in success in war and business. Because governments do not wish certain entities in and out of their countries that have access to ways to receive and send hidden data that may be a threat to national interests and cryptography has been subject to various restrictions in many countries and ranging from limitations of the usage and export of software to the public dissemination of mathematical concepts that can be used to develop cryptosystems. However, the Internet has allowed the spread of powerful programs and more importantly and the underlying techniques of cryptography.

II. RELATED WORK

In[2] authors used average residual battery level of the entire network and it was calculated by adding two fields to the RREQ packet header of a on-demand routing algorithm i) average residual battery energy of the nodes on the path ii) number of hops that the RREQ packet has passed through.According to their equation retransmission time is proportional to residual battery energy. Those nodes having more battery energy than the average energy will be selected because its retransmission time will be less. Small hop count is selected at the stage when most of the nodes have same retransmission time. Individual battery power of a node is considered as a metric to prolong the network lifetime in [3]. Authors used an optimization function which considers nature of the packet, size of the packet and distance between the nodes, number of hops and transmission time are also considered for optimization. In [4] initial population for Genetic Algorithm has been computed from the multicast group which has a set of paths from source to destination and the calculated lifetime of each path. Lifetime of the path is used as a fitness function. Fitness function will select the highest chromosomes which is having highest lifetime. Cross over and mutation operators are used to enhance the selection. In [5] authors improved AODV protocol by implementing a balanced energy consumption idea into route discovery process. RREQ message will be forwarded when the nodes have sufficient amount of energy to transmit the message otherwise message will be dropped. This condition will be checked with threshold value which is dynamically changing. It allows a node with over used battery to refuse to route the traffic in order to prolong the network life. In [6] Authors had modified the route table of AODV adding power factor field. Only active nodes can take part in rout selection and remaining nodes can be idle. The lifetime of a node is calculated and transmitted along with Hello packets. In [7] authors considered the individual battery power of the node and number of hops, as the large number of hops will help in reducing the range of the transmission power. Route discovery has been done in the same way as being done in on-demand routing algorithms. After packet has been reached to the destination, destination will wait for time δt and collects all the packets. After time δt it calls the optimization function to select the path and send RREP. Optimization function uses the individual node's battery energy; if node is having low energy level then optimization function will not use that node.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

III. PROPOSED ALGORITHM

In online shopping system item selects by customers by using portal and then its directed to the pay on payment page.Online merchant have its own payment system or this can take advantage of third party payment systems such as pay online system, PayPal, Web Money and etc. In payment portal customer submits there credit or debit card details such as credit or debit card number, name on the card and expiry date of the card. Details of information search from shopper vary from one payment gateway to another. For e.g., payment in IRCTC website requires Personal Identification Number (PIN) when paying using debit card whereas shopping in Snap deal or Flipchart requires Visa or Master secure code. In addition to that merchant may required a Card Verification Value code, CVV (CVV2 for Visa, CVC2 for MasterCard), which is an authorizing code in CNP transactions. According to the PCI Data Security Standard, merchants are prohibited from storing

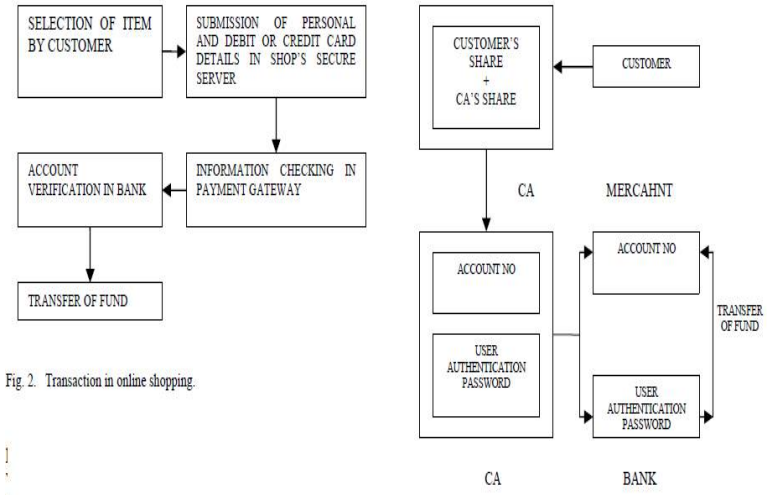


Fig. 2. Transaction in online shopping.

Fig 1: Existing System

Information or PIN data and if it permitted card information such as name, card number and expiration date is stored and certain security standards are required. However recent high profile breaches such as in Epsilon, Heartland Payment Systems and Sony's PlayStation Networks show that card holders' information is at risk both from inside and outside. A solution can be forcing merchant to be a PCI complaint but cost to be a PCI complaint, is huge and the process is complex and time consuming and it will solve part of the problem. One still has to trust the merchant. And its employees not to use card information for their own purposes.

IV. PROPOSED SYSTEM

In this paper, after viewing the proposed system will know the flow of work. There is a Customer which will register on the online shopping. Customer will select items on online shopping websites. When shopping is done for doing payment process the option window will be displayed to the customer. There is one extra option which is "Up load the Image". The Image is Steganograph Image which includes in it the Customer's Debit card number, Bank details etc.The customer details will be check by the server side. One Key value is provided to the Bank for the Decryption process. Then the payment process done. Fund will be transfer in the bank by the customer. Those are the working

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

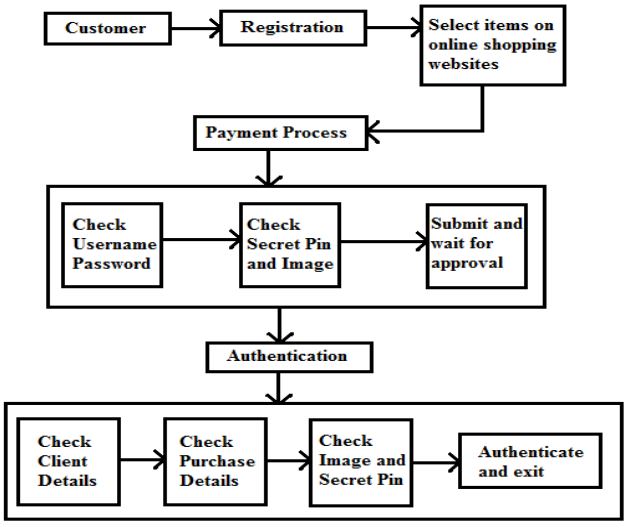


Fig. 2: System Flow

V. ALGORITHM

Effective May 26, 2002 the National Institute of Science and Technology (NIST) has selected a block cipher called RIJNDAEL (named after its creators Vincent Rijmen and Joan Daemen) as the symmetric key encryption algorithm to be used to encrypt sensitive but unclassified American federal information. RIJNDAEL was originally a variable block (16, 24, 32 bytes) and variable key size (16, 24, 32 bytes) encryption algorithm. NIST has however decided to define AES with a block size of 16 bytes while keeping their options open for future changes. 4.0 AES Algorithm.

The more popular and widely adopted symmetric encryption algorithm likely to be encountered now a days is the Advanced Encryption Standard (*AES).* It is found at least six time faster than triple DES. A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow. The features of AES are as follows −

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java.

Operation of AES :-

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs *substitutions* and others involve shuffling bits around *permutations.*

Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix −

Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

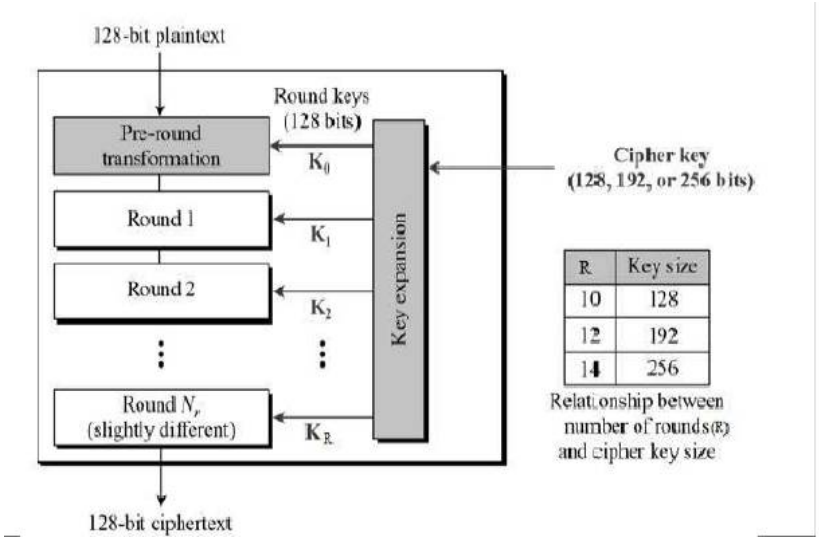
The schematic of AES structure is given in the following illustration –

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

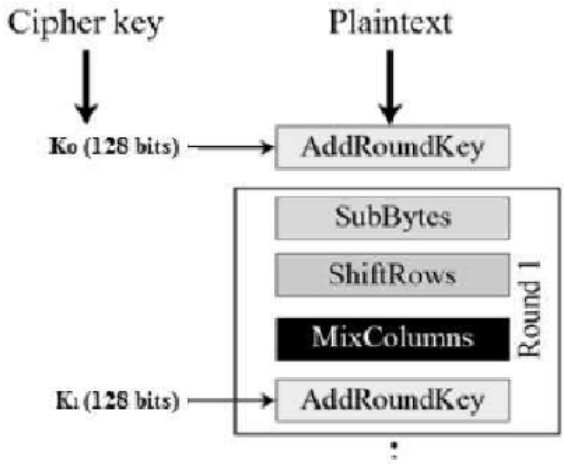
(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016



Encryption Process

Here, we restrict to description of a typical round of AES encryption. Each round comprise of four sub-processes. The first round process is depicted below –



Byte Substitution *Sub Bytes:*

The 16 input bytes are substituted by looking up a fixed table *S – box* given in design. The result is in a matrix of four rows and four columns.

Shift rows:-

Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows –

- First row is not shifted.
- Second row is shifted one *byte* position to the left.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

- Third row is shifted two positions to the left.
- Fourth row is shifted three positions to the left.
- The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

MixColumns:-

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

Addroundkey:-

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the cipher text. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

Decryption Process:-

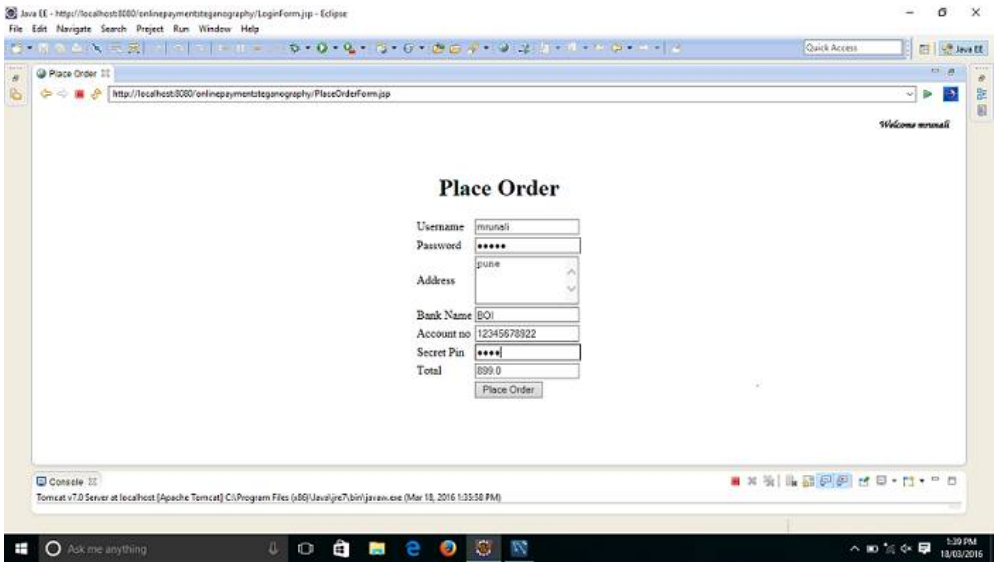
The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order −

- Add round key
- Mix columns
- Shift rows
- Byte substitution

Since sub-processes in each round are in reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithms needs to be separately implemented, although they are very closely related.

Project Execution Screenshot:-

1. **Palce order:-**
   Here after selecting the items we have to fill all the credential details.



ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

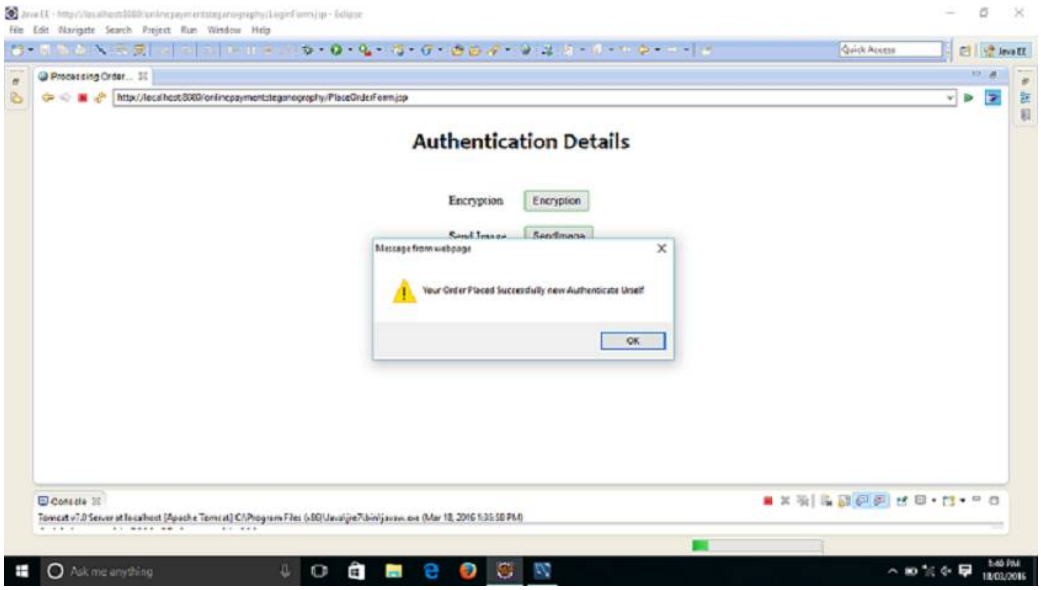
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

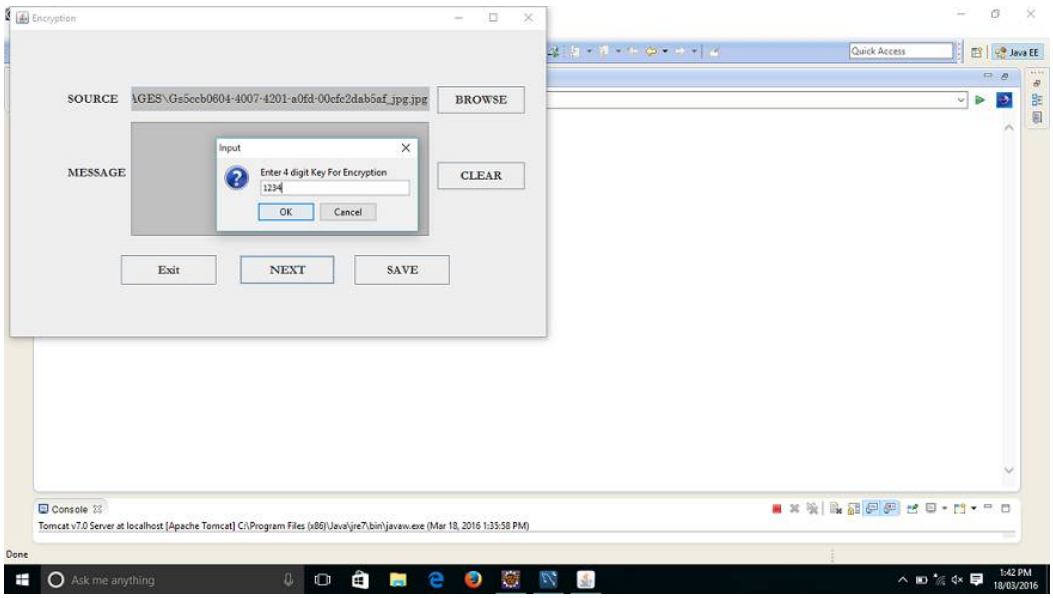
2.Authentication Details:-

In sending this credential details, authentication process will be done by selecting the encryption option.



3.Selecting image:-

Here browse the image which we have to encrypt with secrete key.

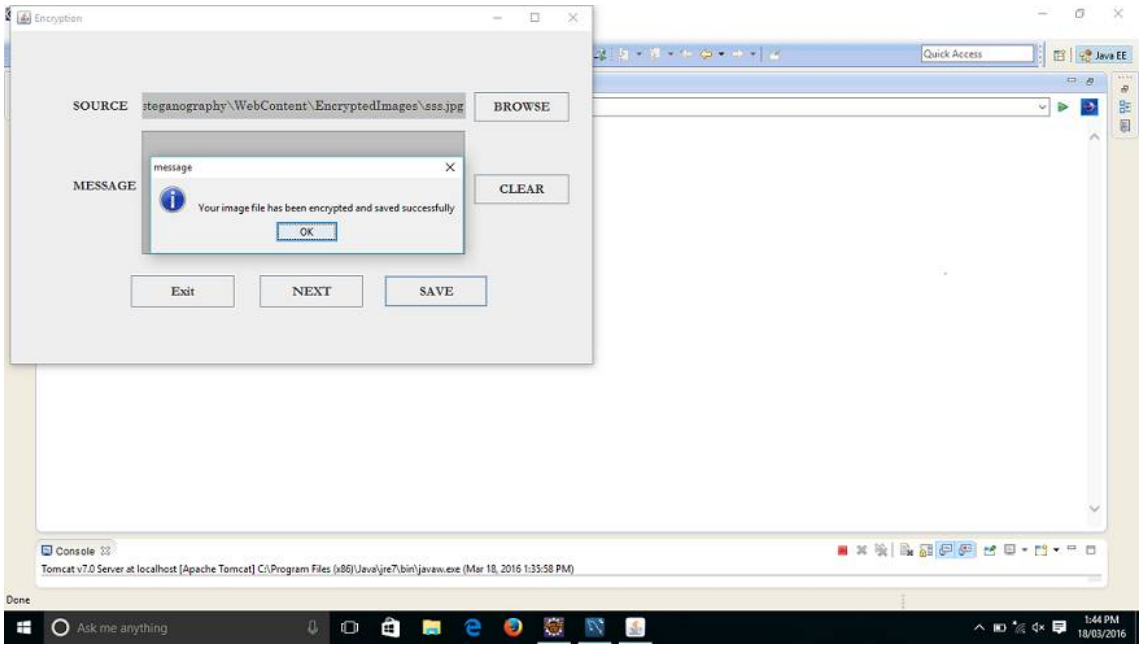


ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

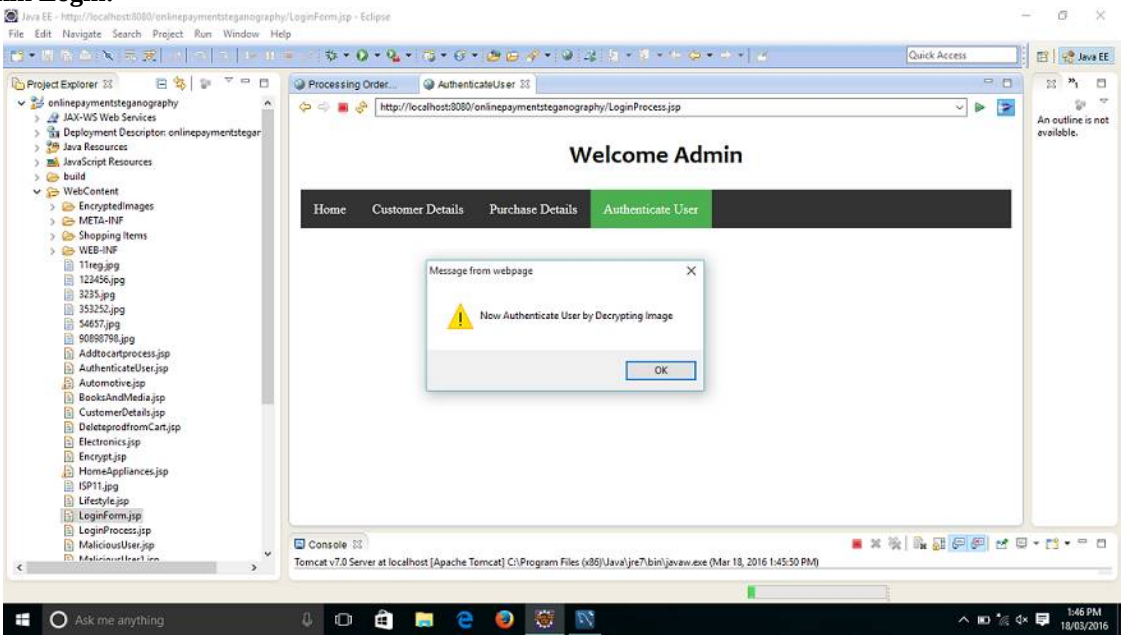
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016



4.Admin Login:-



ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

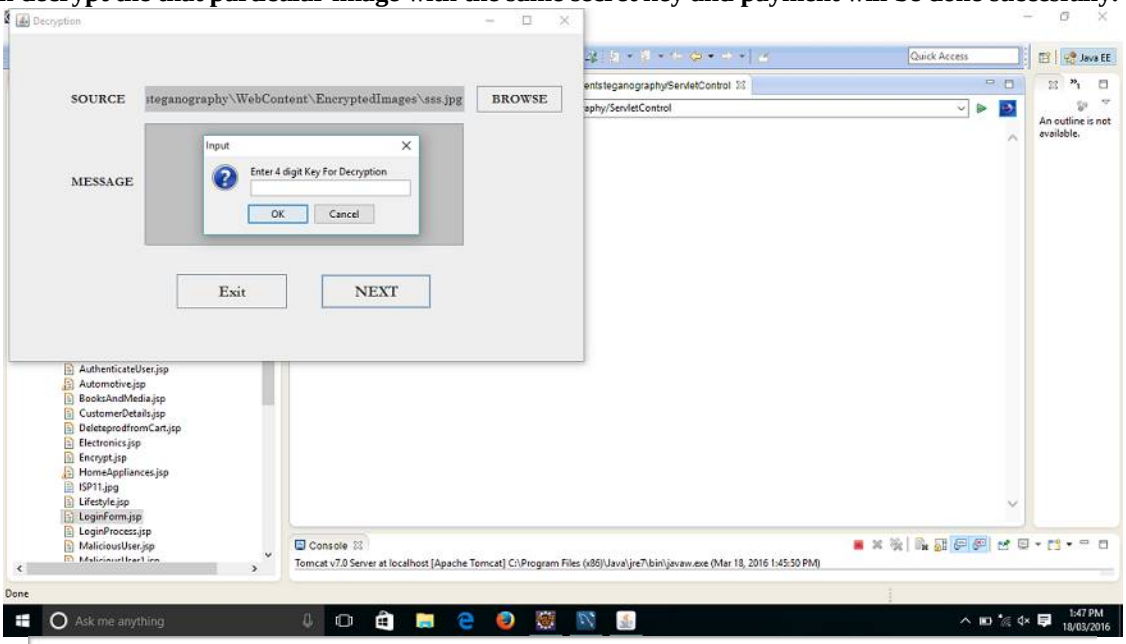
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

5.Decryption process:-

Admin decrypt the that particular image with the same secret key and payment will be done succesfully.



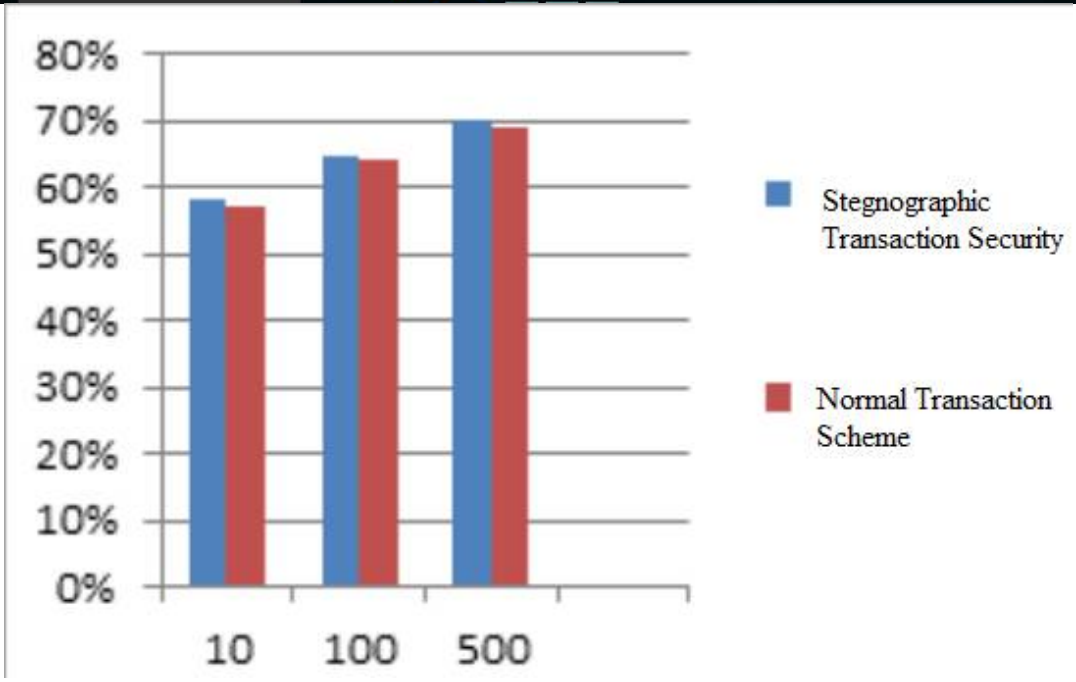


Fig. Comparison of Proposed System and Existing System

A. **EXPERIMENTAL RESULT:**

As Shown in Result graph, our proposed system gives efficient result as compare to existing system. As Compare to Existing System there are major issues in regards to make secure transaction online. In proposed system, we are

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

securing the online transaction by using Steganographic encryption. Credentials of the users get hide into the images while making online transaction. Which is more secure as compare to old transaction methods.

VI. CONCLUSION AND FUTURE WORK

In our paper, a payment system for online shopping is proposed that combines Steganography and visual cryptography and provides customer data not observed and prevents misuse of data by the merchant's side. Steganography is really effective again staves fall and has a high information hiding capacity as compared to traditional steganography approach. The main objective is customer satisfaction and authorized merchant-bank interaction for fund transaction. This method prevent of identity theft and customer data security. In compare to other banking application that uses steganography and visual cryptographyare basically applied for physical banking, the proposed method can be applicable for E-Commerce with interesting areas like payment during online shopping as well as physical banking.

ACKNOWLEDGMENT

We gratefully acknowledge Computer engineering department of Jaihind College of Engineering, Kuran. For technical support and guiding us. We would also like thanks to Prof. S.D.Gunjal and Prof. D.N.Wavhal HOD (Computer Engineering Department) & Guide Prof.A.V.Kanade for their help and dedication toward our project and related study, also our friends for their directly & indirectly help, support and excellent co-operate.

REFERENCES

[1] Jihui Chen, Xiaoyao Xie, 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.
[2] Anti-Phishing Working Group (APWG), "Phishing ActivityTrendReport,2013,"http://docs.apwg.org/reports/apwg_trends_report_q2_2013.
[3] J. Chen, T. S. Chen, M. W. Cheng, "A New Data Hiding Scheme in Binary Image, " Proceeding of Fifth International Symposium on Multimedia Software Engineering, pp. 88-93, 2003.
[4][4] K. Bennet, "Linguistic Steganography: Surevey, Analysis, and Robustness Concerns for Hiding information in Text, " Purdue University, Cerias Tech Report 2004—2013.
[5] J.C. Judge, "Steganography: Past, Present, Future, " SANS Institute, November 30, 2001.
[6] Jaya, Siddharth Malik, Abhinav Aggarwal, Anjali Sardana, "Novel Authentication System Using Visual Cryptography, " Proceedings of 2011 World Congress on Information and Communication Technologies, pp. 1181-1186, Mumbai, India, 2011.
[7] Chetana Hegde, S. Manu, P. Deepa Shenoy, K. R. Venugopal, L M Patnaik, "Secure Authentication using Image Processing and Visual Cryptography for Banking Applications, " Proceedings of 16th International Conference on Advanced Computing and Communications, pp. 65-72, Chennai, India, 2008.
[8] 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.
[9] K. Thamizhchelvy, G. Geetha, "E-Banking Security: Mitigating Online Threats Using Message Authentication Image (MAI) Algorithm," Proceedings of 2012 International Conference on Computing Sciences (ICCS), pp. 276 – 280, 2012.
[10] S. Suryadevara, R. Naaz, Shweta, S. Kapoor, "Visual cryptography Improvises the security of tongue as a biometric in banking system," Proceedings of 2011 2nd International Conference on Computer and Communication Technology (ICCCT), pp. 412 – 415, 2011.
[11] Kalavathi Alla, Dr. R. Siva Rama Prasad, "An Evolution of Hindi Text Steganography," Proceding of Sixth International Conference on Information Technology, pp. 1577-1578, Las Vegas, NV, 2009.
[12] Juan Chen, Chuanxiong Guo, "Online Detection and Prevention of Phishing Attacks," Proceedings of First International Conference on Communications and Networking in China (ChinaCom '06), pp. 1 - 7, Beijing, China, 2006.

BIOGRAPHY

Mrunali V. Kale, Shreya B. Pardeshi, Aniket S. Pardeshiis a students in Computer Department of Jaihind College of Engg.,Kuran ,SPPU,Pune.
Prof. A. V. Kanade ,Department of Computer Engg.,JCOE Kuran,SPPU Pune.