Abstract

In recent time E-Commerce market is rapidly grown in the world. Online shopping has become more popular. Credit or Debit card fraud and information security are major problems for customers, vendors and banks. This work presents a new approach for providing security for personal information during online shopping thereby securing the customer data and high customer confidence and preventing identity stealing. The method uses two types of Cryptography, visual steganography and image slicing. Web based Garment Designing Tool helps the user to design their own clothes and accessories online, it facilitate easy access of online shopping. To design clothes or start a fashion label, designing clothes take thoughts and assurance. It have to be able to envision the outfits design, to draw them, and then to decide the fabric and embroider the clothes that have been dreaming of. So buy product through this site.

1. INTRODUCTION

Online shopping will be revolutionizing the business to making everything to anyone could want available by the simple click of a mouse button [1]. Identity theft[2] and phishing[3] are the common dangers of online shopping. Attackers can pinch and abuse data, leading to
painful disclosure, poor publicity, and fines. In this work, a new method is proposed, that uses two types of Cryptography, visual steganography and image slicing, which reduces information sharing between client and online vendor but enable successful fund transfer from client’s account to vendor’s account thereby securing client personal information and preventing misuse of information at vendor side. The method proposed for E-Commerce but can easily be extended for online banking as well as physical banking.

Web based Garment Designing Tool helps user to design their own garments through online. It facilitates easy access of online shopping. To design clothes or start a fashion label, designing clothes takes imagination and commitment. To envision the outfits to design, to draw them, and then to choose the garment. This proposed system aims that user can design their own clothes such as T-shirts, shirts. Churidar, Sarees and accessories such as cup, bag, cap, and clothes such as T-Shirts, churidars, etc. are stylish, comfortable and liked by all segments of people. It offers customized tee with an option to upload image, text. Instead of asking designers to sketch out free-form designs, this provides a web-based scrapbooking tool that access a large library of fashion pieces. It encourages users to create sets, track other users and inspire each other with fashion find. The site also inspire imagination by hosting design. In the proposed work user can buy so it introduces a new advance for providing restricted information only that is essential for fund transfer throughout online shopping so, safeguarding customer’s data and increasing self-assurance and preventing identity theft technique uses combined function of cryptography and visual steganography for this purpose, and also uses image slicing for more secure.

2. CRYPTOGRAPHY, STEGANOGRAPHY AND IMAGE SLICING

Cryptography [4] is the study of mathematical technique associated to information security such as data integrity, confidentiality, entity verification, and data origin verification. Cryptography helps to protect information by transforming it into an unreadable format. The plaintext or original text, is converted into a coded equivalent called cipher text by an encryption algorithm. Only those have a secret key can decipher (decrypt) the cipher text into plaintext. Cryptography systems can be generally classify into symmetric-key systems and asymmetric-key systems.

Steganography [5] derived from the Greek steganos (covered or secret) and -graph (writing or drawing). Steganography can be defined as the beating of data by embedding messages contained by other messages, images, graphics or sounds.

Image slicing [6] and concatenating, and other image handling techniques are important in parallel computing. It receiving small chunks of an image which can be manipulated parallel. In such a scenario it can be concatenate those chunks together. To split an image imageio package are used.

3. RELATED WORK

The conventional method of online shopping involve customers or client selecting items online shopping portal and direct it to the expense access. Different expense access have different methods of storing detailed data of consumer. The important use of graphic images
might be a trouble to customers with slow internet connection. Initially, the decision was to build a 3D design tool; consider the bandwidth issue, a 2-D design tool was developed instead. The main confront is to present sensible images at satisfactory transfer rate. Creating garments parts and integrating with the system make sure, a match and perfect fit cause another difficult task.

In result to hide 4 letter word, 8 words are required not including the words that are added to provide flexibility in sentence building. So to hide a large message, this technique requires large no of words and create a difficulty in sentence construction. By Applying it to online banking to create spam mail to hide one’s banking information, it use existing pattern blocks to create new styles of garments. It cannot rely on the Payment Procedure.

4. METHODOLOGY

4.1 Methodology of Crypto Analysisto Hide Text

Customer will enter the data to use online payment. Firstly, use blowfish algorithm then stores it in a string and secondly RSA algorithms are used to encrypt data more securely.

4.1.1 Blow Fish Algorithm

It is a symmetric block encryption algorithm designed in consideration with, Fast, Compact, Simple, Secure. It encrypts block data of 64-bits at a time. it will follows the feistily system and this algorithm is classified into two parts: Key-expansion & Data Encryption. Key-expansion: It will translate a key of at most 448 bits into more than a few sub key arrays totalling 4168 bytes. Blowfish use large number of sub keys. These keys are generating before to any data encryption or decryption. Data Encryption having a purpose to iterate 16 times of system. Every round consists of key-dependent variation and a key and data-dependent replacement. All operation is XORs and add-ons 32-bit words. The additional operations are four indexed array data find tables for every round.

Algorithm: Blowfish Encryption

- Divide x into two 32-bit halves: xL, xR
- For i = 1 to 16:
  - xL = XL XOR Pi
  - xR = F(XL) XOR xR
- Swap XL and xR
- Swap XL and xR (Undo the last swap.)
- xR = xR XOR
- xL = xL XOR Pi
- Recombine xL and xR

4.1.2 RSA Algorithm

The public key contains modulus n and the encryption exponent e. The private key contains the modulus n and the decryption exponent d, which must be kept top secret. p, q, and φ(n) must also be kept secret since they can be used to calculate d. An another, used by PKCS#1, is to desire d matching de ≡ 1 (mod λ) with λ = lcm(p − 1, q − 1), where lcm is the least common multiple. By λ instead of φ(n) allow more choice for d. λ can also be define using
the Carmichael function, \( \lambda(n) \). Since any regular factors of \((p-1)\) and \((q-1)\) are present in the factorization of \(p^*q-1\), it is recommended that \((p-1)\) and \((q-1)\) have only very small common factors, if as well the necessary 2.

Equations and formulae must be typed in MathType, and number consecutively with Arabic numerals in parentheses on the right hand side of the page. They must also be separated from the adjacent text by one space.

### 4.2 Data Embedded (Steganography)

![Data Embedded Diagram](image)

**Figure 1. Data embedding**

In figure 1 the Cryptography data’s are embedded or hide in a cover image. It may become more secure. Then the images are sliced [7].

### 4.3 Image Slicing

Image slicing and concatenating and other image manipulation techniques are important in parallel computing. This work uses a pretty straight forward way to split an image using Java imageio package. Firstly read the image file into a class File Input Stream, it contains input bytes from a file in a file system and it is meant for reading streams of raw bytes such as image data. Then object of File Input Stream put on class Buffered Image. A Buffered Image is a kind of class for doing with Images, so you can do anything with a Buffered Image that you can do with an Image. For instance, the Graphics class contains a number of methods for drawing Image objects. Some of these methods take only an X and a Y coordinate at which to draw the image and just draw the image at its original size. It also takes a width and a height and scale the image as appropriate. Then create a Buffered Image array with size of number of images want to slice. Initialize the image array with readied image's height width and type by the help of Buffered Image. Create 2dgraphics in each array elements by Graphics2D, this graphic field are have rectangle of pixels stored in memory. Draw images in this field by draw Image () method of class Buffered Image, draw Image() method in Graphics2D actually operates on a Buffered Image object. This
technique process the specified Buffered Image as specified by a Buffered Image Op object and then draws the processed image at the specified position. Image processing with Buffered Image Op objects in more detail shortly. The draw Image() method operate on a Buffered Image object instead of an Image object. Finally writing mini images from array into new image files making use of the Image IO utility class of Java. Finally number of sliced images created as per the number of elements in the array.

4.4 Image Retrieval and Data decrypting

![Image Retrieval and Data decrypting](image.png)

The purchasing time user will upload the secured image and enter the secret message then CA will decrypt it first. CA have stored the sliced image. CA will concatenate the sliced image and apply destegano process then the decrypted details will got. Then apply the RSA Decryption Algorithm for decrypting the details then got the string again[8].

5 RESULTS

In this proposed work, data submitted by the client to the online vendor is minimized by providing only minimum information that will only check the payment done by the customer from its bank account. This is achieved by the beginning of a central Certified Authority (CA) and joint application of steganography and visual cryptography. Here the banking registration details is kept in the encrypted format and then embedded in the image that selected by user at registration process. When user doing registration the details of account no, userpin, cardno...etc is first encrypted by blowfish encryption method and then that encrypted data are again encrypted by asymmetric encryption method like RSA .This encrypted data is used as input to doing steganography. The output after RSA encryption is embedded in to an image that selected by user at registration. This embedded image is sliced into different equal parts and stored at well. The information received by the vendor can be
in the type of account number connected to the card used for shopping. The data will only legalize receipt of payment from authentic customer.

6. CONCLUSION
In this work, a payment system and web based Garment Designing Tool for online garment design is proposed by combining text based cryptography and visual steganography and image slicing, that provides customer data privacy and prevents misuse of data at vendor’s side. The method is concerned only with obstacle of identify stealing and customer data security. In comparison to other payment this work which uses steganography, visual cryptography & image slicing, are basically applied for physical banking, the proposed method can be applied in the area on payment during online shopping as well as physical banking. Web based Garment Designing Tool helps the user to design their own clothes and accessories online, it facilitate easy access of online shopping.

7. REFERENCES
Arya Sudersanan, Reji George:: Privacy Preserved Online Garment Designing Using Cryptography, Visual Steganography & Image Slicing