E-Commerce Transaction Using Visual Cryptography

Sona Josh[1], Sreelakshmi V[2], Hajira Hazeena[3], Binny S[4]

[1]UG – BCA, Kristu Jyoti College of Management and Technology, Changanacherry, Kottayam, Kerala
[2]UG – BCA, Kristu Jyoti College of Management and Technology, Changanacherry, Kottayam, Kerala
[3]UG – BCA, Kristu Jyoti College of Management and Technology, Changanacherry, Kottayam, Kerala
[4]Associate Professor, Computer Department, Kristu Jyoti College of Management and Technology, Changanacherry, Kottayam, Kerala

Abstract
The abstract focuses on the concept of e-commerce transactions using visual cryptography. E-commerce has revolutionized the way businesses operate and has become an integral part of our daily lives. However, the security of online transactions remains a critical concern. Visual cryptography is a technique that allows the secure transmission of images or information through encryption and decryption processes. This abstract explores the potential of visual cryptography in enhancing the security of e-commerce transactions. It discusses the advantages and challenges of using visual cryptography and proposes a framework for implementing this technique in e-commerce platforms. The abstract concludes by highlighting the potential benefits of visual cryptography in ensuring secure and trustworthy e-commerce transactions.

Keywords—Cryptography, eCommerce, decryption and encryption

1. Introduction

E-commerce's ubiquitous use has transformed the way we shop and conduct financial transactions. This ease, however, comes with its own set of security threats, such as debit or credit card fraud and personal information theft. To address these concerns, cutting-edge solutions such as visual cryptography have emerged as a valuable tool for safeguarding sensitive client data during online transactions.

Visual cryptography is a cryptographic technique that partitions a confidential image or message into multiple shares, rendering each share incomprehensible on its own. These distinct shares can then be distributed among the various participants involved in the transaction.

Using visual cryptography in e-commerce transactions provides a secure approach for handling sensitive data. This cryptographic method entails dividing confidential information into multiple shares represented as images. Each share, on its own, does not disclose essential details of the original data. The shares are subsequently distributed among the different entities participating in the e-commerce transaction. Decryption of the original data and successful completion of the transaction necessitate a minimum threshold of shares. When the required shares are combined, the original data can be decrypted, ensuring the e-commerce transaction's security and privacy.

2. Why Visual Cryptography?

Securing e-commerce transactions and safeguarding sensitive information are of utmost importance in the digital marketplace. An innovative method to achieve this objective is through the application of visual cryptography.

Cryptography is the art and science of ensuring secure communication and safeguarding data using mathematical methods and algorithms.

Cryptography holds a fundamental and indispensable position within the realms of computer science and information security. Its core purpose involves the exploration and application of various methods to safeguard communication, data, and information from any unauthorized interference or modifications.

By incorporating visual cryptography into e-commerce transactions, sellers can encrypt critical data, including credit card details, order information, and product images. This encryption process ensures that no single share possesses the ability to unveil the original information. The utilization of distributed encryption significantly heightens security and mitigates the risks of unauthorized access or data breaches. Throughout this secure process, the buyer receives the encrypted shares through various protected channels, such as email or secure messaging platforms. Upon validation, the buyer reassembles the shares to decrypt and authenticate the original information using specialized visual cryptography decryption algorithms.

3. Visual Cryptography utilized in E-commerce Transactions

E-commerce transactions can incorporate visual cryptography as a secure approach to handling sensitive data. Visual cryptography, a cryptographic method designed for encrypting and decrypting visual information, ensures data privacy and security during its transmission.

In e-commerce transactions utilizing visual cryptography, a series of secure steps ensures the protection of sensitive data. Initially, the data is divided into multiple shares using visual cryptography algorithms, preserving confidentiality as individual shares hold no meaningful information about the original data.

Several techniques and algorithms are used in e-commerce transactions that use visual cryptography to assure the secure transfer and storage of critical information. These procedures are summarised below:

1. ***Encryption:*** The first step in visual cryptography is the encryption of the original image. This process converts the image into a format that is secure and cannot be easily deciphered. Various algorithms can be used for image encryption, including:

- Advanced Encryption Standard (AES)
- Data Encryption Standard (DES)
- Rivest Cipher (RC4)

2. ***Share Generation***: After encryption, the original image is divided into shares, which are smaller fragments or pixels of the image. These shares are generated using algorithms like:

- Shamir's Secret Sharing Algorithm
- XOR-based Visual Cryptography Scheme
- Random Grid-based Visual Cryptography Scheme

3. ***Share Embedding***: The shares generated in the previous step are embedded into separate cover images. This embedding process ensures that the shares are hidden within the cover images, making them indistinguishable to the naked eye. Common algorithms used for share embedding include:

- Bit-Plane Complexity Segmentation (BPCS) algorithm
- Random Image Segmentation (RIS) algorithm
- Visual Cryptography based on Error Diffusion (VCED) algorithm

4. ***Image Distribution:*** Once the shares are embedded, the cover images containing the shares are distributed to different parties involved in the e-commerce transaction. This step ensures that no single party has access to the complete information, enhancing security. Distribution methods can include email, cloud storage, or secure file transfer protocols.

5. ***Image Transmission:*** During image transmission, the cover images are sent securely from the sender to the receiver using encryption protocols like Secure Sockets Layer (SSL), Transport Layer Security (TLS), or Virtual Private Network (VPN). These protocols ensure the confidentiality and integrity of the transmitted data.

6. ***Image Reconstruction:*** Upon receiving the cover images, the shares are extracted and combined to reconstruct the original image. The reconstruction process involves algorithms such as:

- Majority Voting Algorithm
- Exclusive OR (XOR) Algorithm
- Stack Algorithm

7. ***Data Decryption:*** Finally, the reconstructed image is decrypted to retrieve the original information. The decryption process uses the same algorithm that was used for encryption in the first step, ensuring the information is recovered accurately and securely.

These procedures and algorithms ensure the privacy and confidentiality of customer data in e-commerce transactions, making visual cryptography a valuable tool for secure information exchange.

Visual cryptography is practically employed in various aspects of E-commerce security:

- Captcha Generation: During the registration phase, visual cryptography is used to generate captchas, ensuring secure user verification and thwarting automated bots from gaining access to the system.
- Secure Credit Card Data Transmission: Visual cryptography is applied when transmitting a text file containing credit card details from the Merchant Plug-In to the Card Provider Directory Server. This involves splitting the sensitive information into shares, thereby enhancing data protection during the transmission process.
- Enhanced One-Time Password (OTP) Authorization: Visual cryptography is employed in generating Quick Response Codes (QR codes) containing One-Time Passwords (OTPs) for authorizing payment transactions. By dividing the OTP into shares, the security of the authorization process is significantly bolstered.

Real-time collaboration among entities allows secure share combination and decryption without directly sharing the sensitive data, thus safeguarding against data breaches and unauthorized access. Visual cryptography proves to be a robust approach for ensuring secure e-commerce transactions while upholding the principles of confidentiality and data integrity.

4. Pros & Cons

Visual cryptography proves to be a reliable and effective approach for conducting cryptographic transactions within the domain of ecommerce.

4.1. Advantages:

- Enhanced Security: Sharing sensitive information across parties, preventing unlawful interception and decryption, and assuring customer data safety are all ways that visual cryptography improves security.
- User-Friendly: Visual cryptography's user-friendliness comes from using images, simplifying transactions without complex algorithms or technical expertise.
- Decentralized Trust Model: The advantage of visual cryptography is its decentralized trust model, which involves numerous participants in decryption, does not require a central authority, and ensures trustworthiness.
- Swift and Efficient: The quick and effective technique of visual cryptography, free from complicated computations, guarantees smooth and enjoyable ecommerce transaction experiences.
- Versatility: Visual cryptography's versatility handles diverse data types, from plain text to multimedia content, making it suitable for various ecommerce applications.

While visual cryptography offers several advantages for ecommerce transactions, it also has some potential demerits:

4.2. *Demerits:*

- Complexity: Compared to conventional methods, visual cryptography can be more complicated because it calls for careful share management and design.
- Share Management: Securely managing and distributing shares among multiple parties can be challenging, especially in large-scale ecommerce systems with many participants.
- Increased Bandwidth Usage: Visual cryptography's larger data transmission compared to traditional methods may result in increased bandwidth usage during ecommerce transactions.
- Reduced Efficiency for Large Data: For huge data sets, visual cryptography can lose effectiveness as the size and number of shares grow.
- Limited Error Tolerance: Errors during the encryption or decryption process can significantly affect the quality of the shares, leading to potential data loss or corruption.

5. Conclusion

To sum up, visual cryptography presents a highly promising method for ensuring the security of E-Commerce transactions. It effectively tackles security challenges by guaranteeing confidentiality, safeguarding data privacy, and preventing unauthorized access during online transactions.

Nonetheless, it is crucial to adopt a comprehensive security approach, which involves implementing secure communication protocols, regular software updates, and robust authentication mechanisms. By doing so, users will develop trust in the system, leading to the sustainable growth of E-Commerce in the digital age.

6. References:

1) https://en.m.wikipedia.org/wiki/Visual_cryptography
2) https://en.m.wikipedia.org/wiki/E-commerce
3) http://www.ijarcs.info/index.php/Ijarcs/article/view/3057
4) https://www.sciencedirect.com/science/article/pii/S2212017316302559
5) https://ijarcce.com/upload/2018/march-18/IJARCCE%2077.pdf
6) https://www.ijert.org/research/approach-for-secure-onlinetransaction-using-visual-cryptography-text-steganography-IJERTV4IS030775.pdf
7) “Online Fraud Transaction Prevention System Using Extended Visual Cryptography and QR Code” By Shubhangi Khaimar1 and Reena Kharta, Department of Computer Engineering, Pimpri Chinchwad College of Engineering, Pune-44, India.2017 IEEE.
8) “Enhanced password Processing Scheme Based On Visual Cryptography and OCR” By Dana Yang, Inshil Doh and Kijoon Chae, Dept. Computer Science and Engineering Ewha Womans University Seoul, Korea. 2017 IEEE.
9) Online Payment System Using Visual Cryptography and Steganography “By Souvik Roy1 and P. Venkateshwaran2, Department of Electronics & Telecommunication Engineering, Jadaypur University, Kolkata-700032, India. 2016 Online International Conference on Green Engineering and Technologies (IC-GET). 55500
10) Pakshwar, Rinki, Vijay Kumar Trivedi and Vineet Richhariya. "A survey on different image encryption and decryption techniques.", IJCSIT) International Journal of Computer Science and Information Technologies 4.1, 2013.
11) Kumar, M. Arun, and K. Jhon Singh, "Novel Secure Technique using Visual Cryptography and Advance AES for images.", International Journal of Knowledge Management and e-learning, Vol. 3, No. 1, pp. 29-34, 2011.