International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Secure Data Transaction Using Steganographic Methods

Sherin B[1] , Prof Miriam Thomas[2], Dr.T.Mahalekshmi[3]

[1]Final year Student, Sree Narayana Institute of Technology Kollam, Kerala, sherinmcasnit@gmail.com
[2] Assistant Professor, Sree Narayana Institute of Technology,Kollam,Kerala, miriam@gmail.com
[3] Principal, Sree Narayana Institute of Technology,Kollam,Kerala, mlakshmi.t@gmail.com

ABSTRACT

Banking sector is one of the major sectors where security plays an important role. Currently India is focusing on to move to cash less economy where bank plays an important role in transaction. On depending more on banks, the security issues in this sector also raises rapidly. Many intruders are trying to break into the system here comes the importance of our system. In our system bank will upload the image with the user relevant data. Then the details of the users will be embedded to the user image, then this will be encrypted. So, this encrypted image will have the image and the details as encrypted form. Then the transmission between the banks or for processing any request these encrypted image will be passed. Each module will have provision to view the details of user or bank according to their preference. On receiving side, the data is decrypted then decoded to obtain the initial image and the data.

Index Terms— embedded, encrypting; encoding; image decode;

INTRODUCTION

With the rapid advancement of internet and wireless network technology, picture encryption is becoming increasingly important in order to ensure the integrity and validity of digital images during network transmission and to prevent malicious tampering or forgery.According to the different work domains, the common digital image encryption algorithm is currently divided into spatial domain and transform domain algorithms. In the spatial domain image encryption technology AES image encryption is used, this kind of algorithm is easy to implement. AES decryption algorithm is used to decrypt the image. Recently, the development of information technology and communication technology is very significant. Image, which is as a carrier of information, is widely used.However, because the digital image data is so huge, we must compress it in order to store and send it. Image compression technology has advanced rapidly in recent years, and necessary international standardisation is nearing completion. Many researchers are committed to research this area. They hope to come up with efficient coding schemes to meet the needs of different applications. It can be said that the highly efficient method of image coding will continue to be the most advanced technology. In this paper, we introduce the pixel pairing algorithm technology for data hiding. According to the literature, we propose an image compression scheme based on harmonic inpainting model which amount to minimizing the square value of the gradient of the image. Compared with other compression schemes, our scheme has two features. In encoding, we only encode edge extension image to achieve a high compression rate. The decoding is realized by a harmonic inpainting model to achieve a better quality of reconstructed image.

AESIMAGE ENCRYPTION

ALGORITHM

Image encryption is the process of converting a plain image into an encrypted image (a cypher image). For image encryption, the round includes the following stages: • Substitute Bytes • Shift Row • Mix Columns • Add Round Key Substitute Bytes: Non-linear byte substitution is used in the Sub Bytes transformation, and each of the state bytes is treated separately.This is accomplished by employing the S-box replacement table, which has been pre-calculated. The S-box table comprises 256 numbers (from 0 to 255) and the values they produce. Row Shift: Shift The state's rows are cyclically left shifted as part of the rows modification. Row 0 remains intact, whereas rows 1 and 2 move one byte to the left, two bytes to the left, and three bytes to the left, respectively. mix Columns: In mix Columns transformation, the columns of the state are considered as polynomials over GF () and multiplied by modulo + 1 with a fixed polynomial c(x), given by: c(x)= {03} + {01} + {01}x+ {02}. AddRoundKey: By using a simple bitwise XOR operation, the AddRoundKey transformation adds a Round Key to the State that results from the operation of the mix Columns transformation. Using the Key Expansion technique, each round's Round Key is derived from the main key. A total of fourteen 256-bit Round Keys are required for the encryption and decryption method.

AES IMAGE DECRYPTION:

Reverse of encryption is called decryption. It means conversion of cipher image into plain image. The round consists of the following stage for image decryption.

- Add Round Key
- Inverse Shift Row
- Inverse Substitute Byte
- Inverse Mix Columns

Add Round Key: Add Round Key is its own inverse function because the XOR function is its own inverse. The round keys have to be selected in reverse order.

Inverse Shift Row: Inv Shift Rows exactly functions the same as Shift Rows, only in the opposite direction. The first row is not shifted, while the second, third and fourth rows are shifted right by one, two and three bytes respectively.

Inverse Substitute Byte: The Inv Sub Bytes transformation is done using a oncepre calculated substitution table called InvS-box. That InvS-box table contains 256 numbers (from 0 to 255) and their corresponding values

Inverse Mix Columns: In the Inv Mix Columns transformation, the polynomials of degree less than 4 over GF(28), which coefficients are the elements in the columns of the state, are multiplied modulo(x4 + 1) by a fixed polynomial d(x) = {0B}x3 +{0D}x2 + {09}x + {0E}, where {0B}, {0D}; {09}, {0E} denote hexadecimal values.

PIXELPAIRING ALGORITHM FOR ENCODING AND DECODING

The technology of embedding hidden data into the medium for clandestine communication is known as information hiding. A tremendous amount of data is transmitted through the Internet due to the rapid expansion of the Internet. Images, audio, and video are currently the most commonly used media for data concealing, with digital picture being the most widely employed. For the past decade, researchers have been quite interested in image steganography. LSB replacement is one of the most often used steganographic techniques, taking use of the fact that the human visual system is unaffected by minor changes in pixels and that the low bit plane of the pixel contributes very little to image quality. However, for even pixels, this approach can only add 1 or remain unchanged, while for odd pixels, it can only drop 1 or remain unchanged. As a result of the imbalanced embedding distortion, the images suffer from histogram assault. Chan et al. proposed an optima pixel adjustment procedure (OPAP) approach for reducing the distortion induced by least significant bit (LSB) embedding by adjusting the pixels. To embed a hidden message, both the LSB and OPAP systems used one pixel as an embedding unit. Methods for B-ary secret information embedding employing two or more pixels as a basic unit were proposed as steganography progressed. This type of stenographic algorithm can increase the image quality pixel by pixel. However, for even pixels, this approach can only add 1 or remain unchanged, while for odd pixels, it can only drop 1 or remain unchanged.

RELATED WORKS

Mazen El Maraghy et al. used the AES-128 bit method to optimise area and speed in their study. They employed a 128-bit data set and a 128-bit encryption key. In real time, the implemented hardware design is evaluated. For speed, power consumption, and area, M.Sambasiva Reddy et al. employed the identical AES-128 bit algorithm. They used EDK to implement the AES algorithm. Trang, Hoang et al. This results in a low-complexity design that achieves low latency and high throughput with ease. The design employed an iterative looping technique with a 128-bit block and key size, as well as an S-box lookup table implementation. To reflect a high level of security and improved image encryption, Kamali S.H et al. applied a modified advanced encryption technique. The Shift Row Transformation is adjusted to make the change. The results of the previous AES algorithm and the modified AES algorithm were compared by the author.

EXISTING SYSTEM

The insecurity in sending information may cause the intruders to attack the data. Many economic losses may occur due to this. Confidential information may leak and will adversely affect the user and also the bank.

Disadvantages of existing system

Some of the disadvantages of the existing system are as follows:

- There is no mechanism to securely send the bank's data.
- Attacks are high in the existing systems.
- Many systems are not trustworthy.

PROPOSED SYSTEM

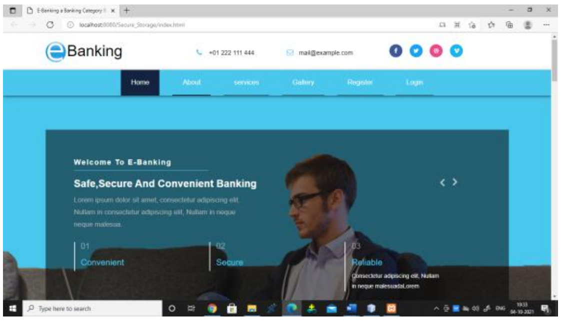
In proposed system, in order to provide more security to confidential data we are using four algorithms that is for encryption, decryption, encoding and decoding. The data is first encoded inside the image and it is encrypted then send to the receiver side, it is then decrypted and decoded by the receiver.

Provide more integrity by the use of AES image encryption decryption algorithm and pixel pairing algorithms.This provides a user-friendly interface there by avoiding the confusing scenarios.

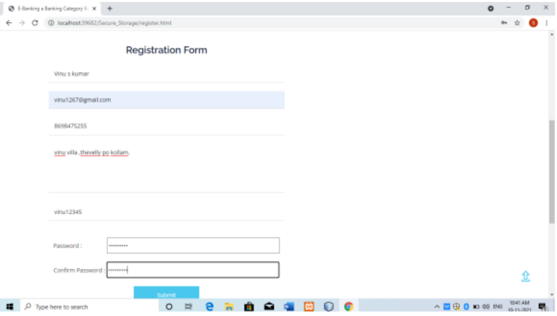
Advantages of proposed system

- Userfriendly.
- Provide more security.
- Provide integrity.
- Avoid confusing scenario.

RESULTS


localhost:8080/Secure_Storage/index.html
eBanking
+01 222 111 444
mail@example.com
Home
About
services
Gallery
Register
Login
Welcome To E-Banking
Safe,Secure And Convenient Banking
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nullam in consectetur adipiscing elit, Nullam in neque neque malesua.
01 Convenient
02 Secure
03 Reliable
Consectetur adipiscing elit, Nullam in neque malesuadaLorem
Type here to search

HOME PAGE



Registration Form

Vinu s kumar

vinu1267@gmail.com

8698475255

vinu villa ,thevelly po kollam.

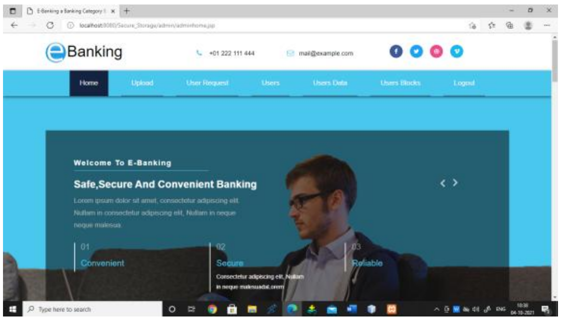
vinu12345

Password : ••••••••

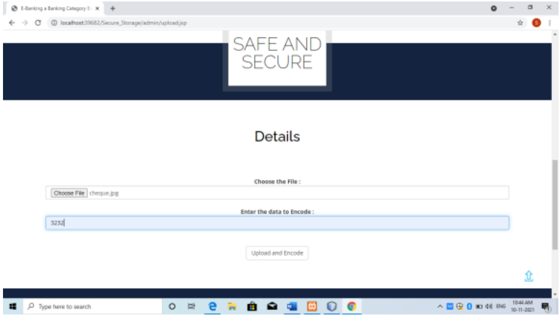
Confirm Password : ••••••••

Submit

USER SIGN-UP


localhost:8080/Secure_Storage/admin/adminhome.jsp
eBanking
+01 222 111 444
mail@example.com
Home
Upload
User Request
Users
Users Data
Users Blocks
Logout
Welcome To E-Banking
Safe,Secure And Convenient Banking
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nullam in consectetur adipiscing elit, Nullam in neque neque malesua.
01 Convenient
02 Secure
03 Reliable
Consectetur adipiscing elit, Nullam in neque malesuadaLorem
Type here to search

ADMIN HOME PAGE



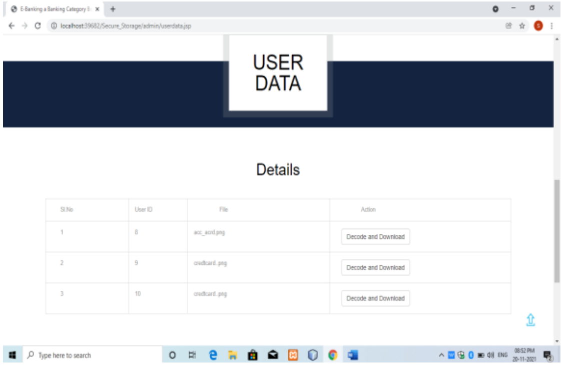
Details

Choose the File : Choose File cheque.jpg

Enter the data to Encode : 3232

Upload and Encode

UPLOADING PAGE


E-Banking a Banking Category B
localhost:39682/Secure_Storage/admin/userdata.jsp
Type here to search
08:52 PM
20-11-2021

USER DATA

Details

Sl.No	User ID	File	Action
1	8	acc_acrd.png	Decode and Download
2	9	creditcard..png	Decode and Download
3	10	creditcard..png	Decode and Download

USER DATA

CONCLUSION

Decoding algorithm, based on the AES image encryption and decryption method and the pixel pairing technique, is used to encode and the process of decoding is the inverse of encoding. The picture sensitivity and resilience are also assessed for the experiment outcomes of image encryption and decryption, encoding, and decoding. The results of the simulation experiments show that the proposed system has a high sensitivity to initial images and data, that the algorithm is effective for image encryption, that the decrypted image has small distortion and a strong ability to resist noise, that the algorithm has good security and robustness, and that the algorithm has some practical value in the transmission of digital images.

REFERENCES

[1]htt://ieeexplore.iee.org/document/
[2]https://nevonprojects.com
[3]https://stackoverflow.com
[4]https://en.m.wikipedia.org