Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

December 2014, pg.30 – 33

NATIONAL CONFERENCE ON ADVANCES IN MODERN COMPUTING AND APPLICATION TRENDS
TECHMAN-14
5th & 6th December, 2014, Organized by Acharya Institute of Technology, Bangalore, India

Message Secured Module using Image Cryptography

Manoj Mukherjee[1], Sawata Adya[2], Mrinal Sarkar[3]

Department of MCA, Acharya Institute of Technology, Bangalore

Abstract— Text messaging via mobile devices has become a general means of communication within our culture and workplace. The smartphone usage among people is increasing rapidly and with the phenomenal growth of smartphone use for messaging. Message security is a most important issue and message hiding with image cryptography is one of the possible ways to ensure the security of the important message from out sider. This paper proposes a smartphone application that encrypts the message such a way that it is hidden in a combination of Image as well as the Key. The proposed technique uses encryption process that is fully based on Binary data as well as our proposed methodology. Its provide keeps your data protected from outsiders. The proposed model is validated by the prototype implementation in Android platform.

Keywords— Encryption, Message security, image cryptography, Binary data

I. INTRODUCTION

Nowadays, usage of mobile has become a vital part of day-to-day activities of people. We can refer the current time as the era of Smartphones. Messaging is important part for communication each through smartphone via internet so, Message Security is a most important issue in communication and encryption is one of the ways to ensure security of the communicated message. Secure Messages are encrypted bidirectionally and are stored on a network or internet server.

Encoding is the transformation of data into some unreadable form. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended. Decoding is the reverse of encoding; it is the transformation of encrypted data back into some intelligible form. Cryptography is popularly known as the study of encoding and decoding private massages. In cryptography, encryption processes are used in transforming information using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information. The reverse process is referred to as decryption [1].

A. Image Processing

It generally refers to processing of a two-dimensional picture by a digital computer. A digital image is a representation of a two-dimensional image as a finite set of digital values, called picture elements or pixels.

Pixel values typically represent gray levels, colours, heights, two major tasks, Improvement of pictorial information for human interpretation, Processing of image data for storage, transmission and representation for autonomous machine perception. Where image processing ends and fields such as image analysis and computer vision start. Our proposed method is one of the techniques used to encrypt the images by dividing the original image into transparencies. The transparencies can be sent to the intended person, and at the other end the transparencies received person can decrypt the transparencies using our decryption method and key image, thus gets the original message. Our application MSM is a "Message Secured Module" that keeps your data protected from outsiders. Since all message service providers keep all the actual messages in the server as it is, the service providers can access it. Though the data is encrypted after passing the message in the Server-side only, the provider will definitely have the encryption algorithm and they can prey on actual data. Our main purpose is to keep the encryption/decryption algorithm as well as the actual data safe from both the Hackers and the Service Providers.

II. OBJECTIVES

Send confidential data to the receiver in a secured way. Actual data (text, image, video and audio) is encrypted so that it gets protected from outsiders. Since the data is encrypted/decrypted by the MSM app, thus even the providers will not have the algorithm to prey on actual data. Thus the data is protected from Hackers as well as Service Providers. As both the encryption and decryption is done by the MSM App itself (at client side), thus it reduces the work-load at server side. Let MSM app be used by casual/non-tech users and business peoples.

III. METHODOLOGY

What if the providers don't have the algorithm to encrypt/decrypt the message?

This is what the MSM does. It does mot passes the actual message to the Server, rather it encrypts the message locally and send the encrypted data to server. MSM stores the encrypted data in the cloud (not the actual message or algorithm) and only an image is given to receiver via any other medium. We let the hackers play with the image only, neither with the algorithm nor even the message.

- A. Read Image and Text
- B. Calculate length of Text
- C. Convert image to Base64 string. Obtain the substring upto length. and Encode Text string to Base64 and add.
- D. Store Encoded base64 in the server.

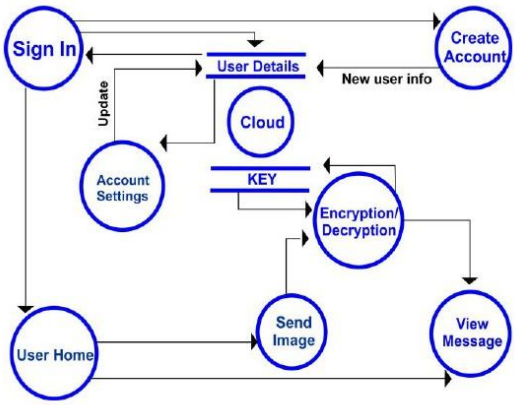
IV. DECRYPTION PROCESS

- A. Read image.
- Fetch the encoded string from server
- c. Convert image to base64 and split.
- encoded string- image spilt base64 string
- e. decode the base64 string to Text
- f. show the message.

V. ALGORITHM

A. Encryption

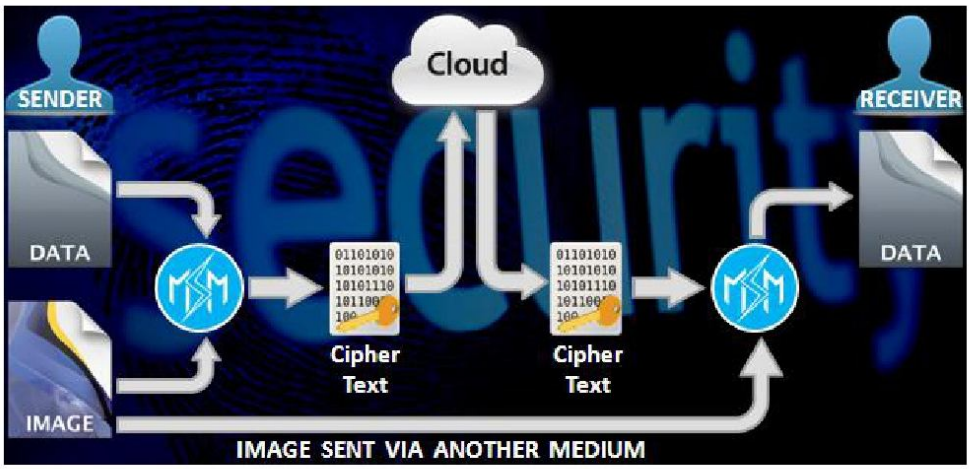
1. START
2. M -> Read a text message from user.
3. I -> Read a image from user
4. N -> Calculate the length of the message
5. IB -> Encoding base64(I)
6. SIB -> substring(IB,N)
7. Ascii_SIB -> convert substring of image to ascii
8. Ascii_M -> convert the massage to Ascii
9. Result -> Ascii_SIB+Ascii_M
10. encode_R -> Encode base64(Result)
11. STOP



B. Decryption

1. START
2. D -> Read The Encrypted text from Server
3. I -> Image read from user
4. N -> find length of Encrypted text
5. CI -> convert image to base64 ie encode_base64(I)
6. S_CI -> subString(CI,N)
7. Ascii_S_CI-> Convert to Ascii of S_CI
8. Decode_D -> Decode the Encrypted Text Decode_Base64(D)
9. AScii_original -> Decode_D-Ascii_S_CI
10. original_Text -> conver ascii to string.

VI. RESULT AND ANALYSIS



VII. CONCLUSION

In this paper we proposed a novel technique that encrypts the message such a way that it is hidden in a combination of Image as well as the Key. The proposed technique uses encryption process that is fully based on Binary data as well as our own Encryption Algorithm. This application can be widely used in Media, Banks, Online transactions and Insurance companies.

REFERENCES

[1] A. Sinkov, Elementary Cryptanalysis: A Mathematical Approach, Mathematical Association of America, 1966.
[2] G. R. Blakely, "Safeguarding cryptographic keys," in Proc. National Computer Conf., vol. 48, pp. 313–317.
[3] Z. G. Ma and S. S. Qiu, "An image cryptosystem based on general cat map," J. China Inst. Commun., vol. 24, pp. 51-57, 2003.
[4] T. Kong and Z. Dan, "A new anti-arnold transform algorithm," J. Software, vol. 15, pp. 1558-1564, 2004.
[5] C. Y. Hong and W. G. Zou, "Digital image scrambling technology based on three dimensions arnoldtransform and its period," J. Nanchang Univ. Nat. Sci., vol. 29, pp. 619-621, 2005
[6] Z. H, "On the period of 2D Random matrix scrambling transform and its application in image hiding," Chinese J. Comput., vol. 29, pp. 2218-2225, 2006.

