

An Android Application Development for Image Watermarking using QR Code

Shital Pawar¹, Rifat Shaikh², Poonam Navale³, Ritika Dhawkhre⁴ and Shalini Kamble⁵

¹⁻⁵Department of Computer Engineering, Bharati Vidyapeeth's College of Engineering for Women, Pune, India
Email: shitalp16@gmail.com, shaikhrifat24@gmail.com, navalep28@gmail.com, ritika4563@gmail.com

Abstract—Digital image security and rectitude are the top major issues in today's informative world. Water marking is a specific method that is used for copyright protection and firm verified. Watermark should be strong and gradual. Digital image watermarking is an embedding data such as an image converting into digital signal using a strong media QR code. It is very difficult to analyse the digital image watermarking has applied to data. This is a competent way to prevent illegal copyright from the modern multimedia network with modern technology in printing and scanning, creating imitate documents which has become a difficult task that makes it very complicated to understand between actual and artificial. So, it is a very big challenge for serving security or digital data. This paper put forward an idea or proclamation to provide and innovative method to verify a digital document. The advanced method of QR code is brought here which permits us to embed a digital data such as an image in QR code. In this paper we bring up and innovative method where the image is encoded in QR that is code in encoded method. If a hacker tried to modify or meddle with the data then he/she will fail to do that so. This is caused because of the encryption key to which the hacker is not aware of it. It is unfeasible to scan or access to the encrypted QR code as the codes are robust.

Index Terms— QR Code, Watermarking, AES (Advanced Encryption Standard) Algorithm, Digital image, Secret key, Decryption and Encryption.

I. INTRODUCTION

We developed an application that tries to protect the end users' authenticity. Because of various attacks are happening in internet world user feel insecure to share their data over a network so we tried to overcome this problem by developing an application which is easy to use and where you can hide your actual data in another form. Digital watermarking is the process of covering message or data it can be in any form like pictures, videos embedded into the signal [1]. It can be related to steganography; in that concept, it will hide messages or data inside a digital signal. It is any famous technique that is used for copyright protection and authentication. Watermark must be strong and inconspicuous. In watermarking we will hide original information in a signal but in steganography, the signal shows no relation to information, and it tries to give guarantee to the end user that important data are never mishandled [2].

Scanned watermarking is useful, it can be used in various places like Watermarks are used in reshaped proof or verification is intolerable in forensics and also trademarked portrayals are bearable. It can be used on any label. Digital Watermarking is a way that authority of digital media is unharmed. It can also fend off copying of data. End-users buy the full version of the product so the video control program also uses the watermarking method in

their system. it can be also used for identification card safety. The Image watermarking process is to fix details of digital such as a sculpture within digital signal using a powerful media QR code. It is burdensome to recognize that digital image watermarking has appeal to the data. This is a suitable way to banned illegal copyrights of data from the collective multimedia transmission. With advanced technology in reproducing and scanning, generate copy documents has become a trouble-free task, it become very difficult to understand between the original and the artificial [3]. Watermarking has been around for several centurial, and can be found in form of a trademark in the papers (logo, text, or pattern). Nevertheless, watermarking or trademarking has been grown for the past 15 -20 years and now can be pre owned in applications [4]. Watermarking the method is split into the following leading steps, implant, charge, insight. Encluse, any algorithm gains the host and information to be flooded and generate a signal

II. MOTIVATION

The main motive behind this is an innovative method to protect the asset of the user or owner through providing security by using Digital Watermarking technique whose work is to protect the authenticity, copyright protection of the owner using a strong media QR code [5]. Desire to provide double security by implementing this technique to overcome the problem of data modification and illegal copyrights Hacker tries to alter, illegal copying or tries to tamper with the data which leads to un-confidentiality of data and insecurity in visible watermarking data as watermarked can be in form of logo or text but in invisible watermark data can present in the form of audio, video [6]. In our paper we cover data inside of any image. End users can use various methods by applying various techniques such as cipher, authentication and firewall we have to male user authentication their data security. for end user satisfaction, we apply basic method of steganography technique and cipher method. In this concept, we find an algorithm for fix the data into image using steganography method which provides the greater safety for sending any particular information or data over a network.

III. RESEARCH GAP

In a recent year, the digital watermarking technique is mostly used with digital media such as image, video, audio, and gif., there are great research and practices to keep the information save and secure nowadays, digital watermark has become very popular, there is enormous transmission growth of multimedia content over the internet network that requires protection mechanism for avoiding modification, tampering, alteration, and copyright infringements of the data [7].Here, are some existing types of digital watermarking: Visible watermark: In this technique the watermarks are visible and the data is hidden inside a multimedia object such that it can be easily seen to a human observer, this contains an important portion of digital data. Invisible watermark: In this technique the watermark is invisible and the data is embedded inside the digital media by steganography method and there are not visible by naked eyes.

Public watermark: This watermark can be easily accessed by the user. It is not much secure as compare to standard watermark it can be easily generated by using any algorithms. Fragile watermark: If fragile watermarks are to be used there must be a system that can detect all the changes [8]. But some disadvantages may cause lethargy these types of watermarks are destroyed by data manipulation. The watermarks that are easily displayed can be modified and remove or override by another watermark. The images with the watermark can be easily resized and cropped. The owner can alter the watermark according to himself so, that means anyone from the sender side can easily manipulate the images. There still needs to be inventions of more robust techniques [9]. There is also a technique has where we can embed our data in an animated image that is GIF. Not only this, the data is embedded by an invisible watermark that cannot be removed or altered under any circumstances; and also verifies the authenticity of the file owner, this is due to cryptography which contains a digital signature that allows anyone to do so. In the market, there are various tools for steganography and watermarks that contribute to all-digital platforms [10]. At present there are also various types of QR code that can used to embed information such as LogoQ is a latest type of QR Code developed to enhance visual assumption by the combination of letters and pictures in complete coloured contents.

Since LogoQ is a highly appreciable type of QR Code, it can easily identify the difference between LogoQ from the regular QR Code. The main motive of LogoQ is the combination of designability and readability [11]. Smartphone requires code dependability. However, there is a restriction that the user must be equipped with smart devices to scan the digital information that is only possible with smart devices that can easily understand the code dependability and technically equipped to do this [12]. Some users, is not too familiar with this

technology. Advertisers have to demonstrate consumers about latest technology to limit doubts. These are some limitations that must be coping up [13].

IV. PROPOSED METHODOLOGY

Intimate Encryption of a data hiding and accessing using QR code authentication system: It is a distinct methodology, where the Image contains embedded QR code which act as a digital media. Then the message which the user wants to send to the receiver is placed in that QR code which is concealed behind the image. After secret key or encryption key will be entered, so that if an intruder tries to alter the message, then he unable do this, as well as there is an image in front and behind the image there is QR code in which message is hidden, message is doubly secured as if any one tries to perceive the message, they unable to do because of the image in front of QR code advantage of this is the image cannot be scanned. The encryption of the message is done using AES Advanced encryption standard encryption algorithm. The encrypted secret message is added inside QR code and the code its self-hidden behind the image. The message can be approach from the QR code and later can be decrypted using Decryption algorithm reverse of AES. After that the message will be retrieved using the secret key which is known to recipient. The data that is transmitting from one user to another is securely reaching to the destination and avoiding un-confidentiality. The working of AES is to encrypt a simple message to become a cipher text, that can be decoded back to the original content by using usual private key. The cipher text gives no clue to the original plain text. The AES are deployed on bytes instead of bits therefore, 128 bits of plain text is assumed as 16 bytes. The QR code used in this implementation is of version 2 that consist of 25x25 matrix. The following line is the method to add QR code

```
QRGEncoder qrgEncoder = new QRGEncoder(inputValue, null, QRGContents.Type.TEXT, smallerDimension);
```

The AES algorithm for embedding the data in QR code a hiding it inside an image which provides security pattern for sending message through a network Cipher text is obtained when AES encodes plain text which can be decoded to the original plain text by using usual private key. It can be seen the cipher text is much different from and gives no indication to the original plain text. We have implemented this project by developing an application using android studio and java platform. An android application is designed that will consider the plain text as message and key required by the AES algorithm and provide the required cipher text at the sender site. The encrypted text then can be decrypted using the application to retrieve the original contents. For encryption: `String encryptedMsg = AESCrypt.encrypt(pwd, message);` and for decryption: `StringdecryptMsg=AESCrypt.decrypt(pwd, encryptedMsg);` methods are used. For Login page we have created a database by using firebase database console that must be associated with android studio that means first you need to register your application with firebase project.

V. PROPOSED ARCHITECTURE

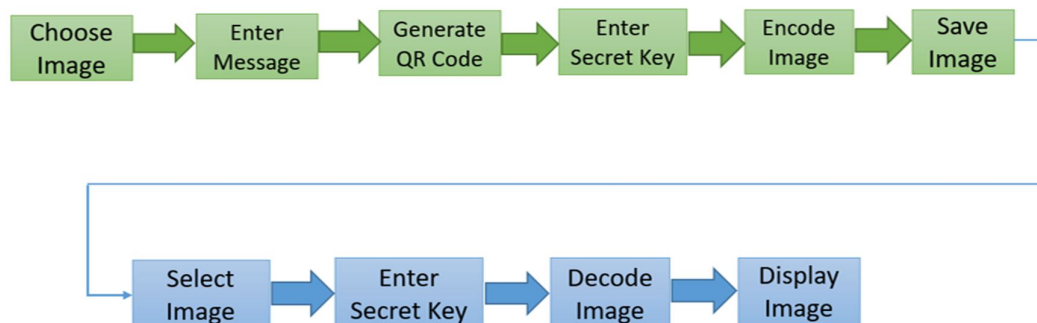


Fig 1: System Architecture

In the above System architecture, the flow shows the process of the application, here the first part is of encoding procedure. The following are the steps for encoding:

1. Choose the image that you want to encode then enter the secret message.
2. Generate the QR code by clicking on "QR Code" button.
3. The most important, enter the secrete key.
4. Click on encode button, the image will be encoded.

5. Save the image by clicking on save button.

Provide the same secret key and the image to the receiver, so that he can decode the content and have access to it by following decoding procedure. The following is the process for decoding:

1. Choose the image that is provided by the sender.

2. Enter the secret key which will be known to authorised user that is sender and the receiver.

3. Decode the image by clicking on “Decode Image” button.

4. After entering the correct secret key the message will be displayed. In some case, if user provide incorrect secret key, then error message will be displayed as “Wrong Secret Key” and if user chooses incorrect image, then “Wrong Image Chosen” error message will be displayed.

VI. RESULTS AND DISCUSSION

This section presents results of experiments performed to evaluate the proposed Image watermarking using QR code technique. The experiments were performed using the Android studio to reduce un-authorized access and provide better security during message transmission. To meet the requirements, the simple and basic approach of image watermarking, encryption and decryption techniques. The AES algorithm for embedding the data in QR code a hiding it inside an image which provides security pattern for sending message through a network Cipher text is obtained when AES encodes plain text which can be decoded back to the original plain text by using usual private key. It can be seen the cipher text is much different from and gives no indication to the original plain text. We have implemented this project by developing an application using android studio and java platform. The information given below is how our application runs:

1. Register to an account if not have an account.
2. Login to your account
3. Authentication Success then click on the encode button.
4. Click on the choose image button, type the
5. The message which you want to send to the Recipient.
6. Click on the Generate QR code and then type the secret key which will be know the recipient and click on the Encode and then save image.
7. Then click on the decode image button, at the recipient side type secret key which is known to the recipient then click on the Decode button.
8. If recipient enters incorrect secret key "Wrong secret key" error will be display.
9. If recipient chooses incorrect image "No message found" error will be display.

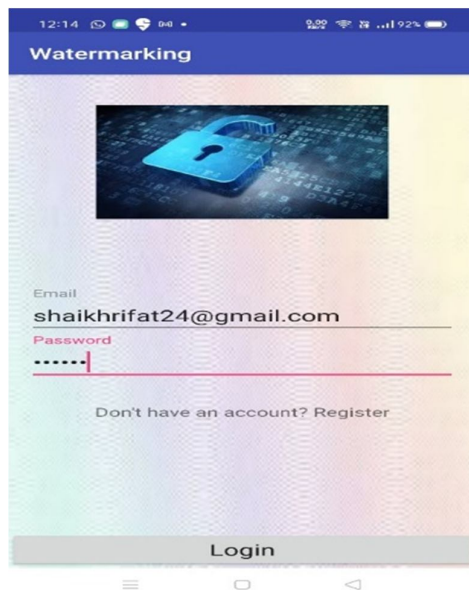


Fig:2: Register to an account

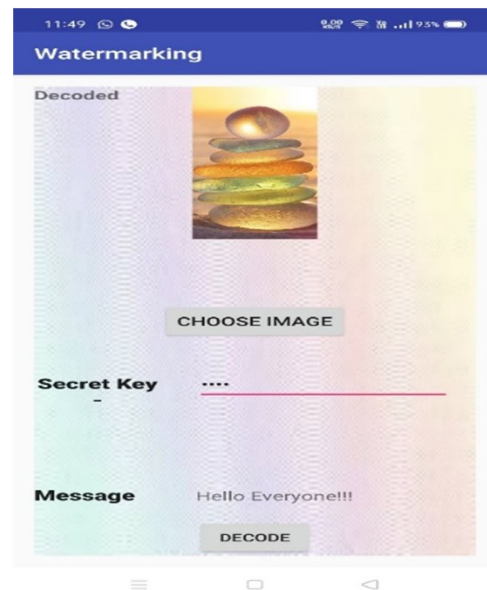


Fig: 3: Login to your account

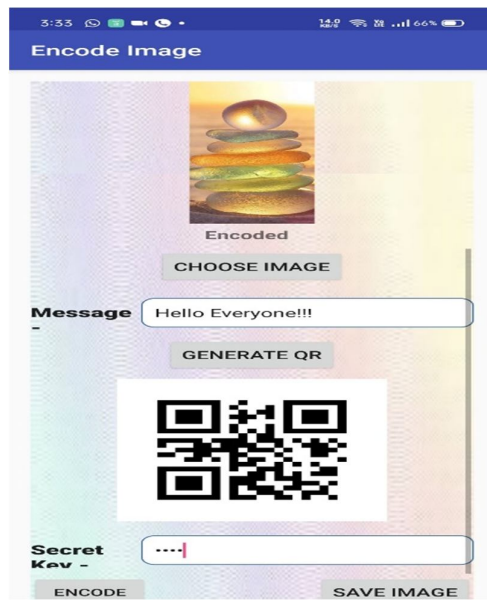


Fig. 4: Decoding

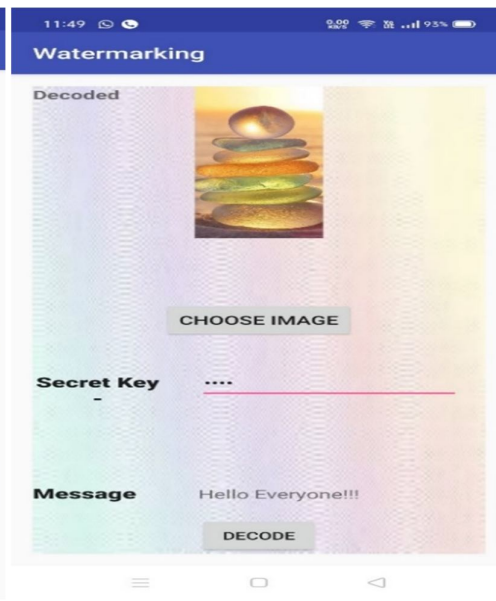


Fig.5: Encoding

A new technology after of digitizing information were developed, a plenty of databases of texts, images, scientific data, video, audio files and other digital information had been appeared in the world. With developing network and internet technologies and connecting computers into the World Wide Web, databases become available for authorize access but for illegal access also. A lot more digital data can be accessed to via network now a days. The problem of data protection is one of the most important. The methods of coding and hiding information are well known from past times as a cryptography and steganography.

VII. CONCLUSION

The advanced solution to protect the asset of the users is to provide security by using the technique image watermarking using QR code, whose work is to protect the legitimacy, copyright protection of owner using a strong media QR code. In addition to, the QR code is also concealed behind the image so that the person observing it will not be able to recognize that, the image contains QR code. In image watermarking technique, the data is embedded in a code structure that is in imperceptibly watermarking. The discussion above is the properties of watermarking technique that demonstrate AES (Advanced Encryption Standard) provides more protection (it is less liable to cryptanalysis than 3DES).

REFERENCES

- [1] M. Manimekalai , R. Bakkiyalakshmi "Hide and Seek: A New Way to Hide Encrypted Data in QR Code Using the Concepts Steganography and Cryptography", Vol. 6, Issue 6, June 2017.
- [2] Mohammed A. Saleh, Image Steganography Techniques - A Review Paper, Vol. 7, Issue 9, September 2018.
- [3] Lalit Kumar Saini, Vishal Shrivastava "A Survey of Digital Watermarking Techniques and its Applications ",2014.
- [4] Oleg Evsutin, Anna Melman and Roman Meshcheryakov, "Digital Steganography and Watermarking for Digital Images" date of publication September 8, 2020.
- [5] Tahera Akhtar Laskar and K. Hemachandran, "Digital Image Watermarking Techniques and Its Applications", IJERT, Vol. 2 Issue 3, pp.2278-0181,2013.
- [6] Saivya Gulati and Daughy Sharma, "SMS Encryption Using AES On Android Application", IRJUIT, pp. SP17335,2018.
- [7] Y. Chow, W. Susilo, J. Tonien, E. Vlahu-Gjorgievska, and G. Yang. Cooperative secret sharing using QR codes and symmetric keys. Symmetry, 10(4):95, 2018.
- [8] P. P. Thulasidharan and M. S. Nair. {QR} code based blind digital image watermarking with attack detection code. {AEU} - International Journal of Electronics and Communications, 69(7):1074 – 1084, 2015.
- [9] I. Tkachenko, W. Puech, C. Destruel, O. Strauss, J. Gaudin, and C. Guichard. Twolevel QR code for private message sharing and document authentication. IEEE Trans. Information Forensics and Security, 11(3):571–583, 2016.

- [10] Shital Pawar and Shashank Joshi, "Agent Based Testing Tool for Event Driven software", International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue3, pp. 2961-2965.
- [11] Tahera Akhtar Laskar¹, K. Hemachandran Digital Image Watermarking Techniques and Its Applications Vol. 2 Issue 3, March – 2013.
- [12] Payal Kaushal ASRA college of Engineering and Technology, Bhawanigarh, Punjab A Review on Digital Image Watermarking Vol. 4 Issue 12, December-2015.
- [13] Zhaoxiong Meng; Tetsuya; Sumiko Miyata; Hirotosugu Kinoshita "Design Scheme of Copyright Management System based on Digital Watermarking and block Chain" Vol:02 ,June-2018.