International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 03 | Mar 2020 www.irjet.net p-ISSN: 2395-0072

Image Watermarking Using QR Code

Ajit N. Gedam[1], Afiya Papde[2], Pranalee Walunj[3], Rana Shaikh[4] ,Sakshi Kamble[5]

[2,3,4,5]Students, Computer Engineering Department, AISSMS Polytechnic, Pune, Maharastra, India
[1]Ajit N. Gedam Lecturer in Computer Engineering Department, AISSMS Polytechnic, Pune, Maharastra, India

---

Abstract - *Digital image security and integrity are the top prioritized issue in today's information World. Watermarking is a famous technique that is used for copyright protection and authentication. Watermark Should be robust and imperceptible. Digital image watermarking process is to embed information of digital such as an image into digital signal using a strong media QR code. It is very difficult to identify that digital image watermarking has applied to the data This is a competent way to restrict illegal copyrights of Information from interactive multimedia networks.With advanced technology in printing and scanning, creating imitate documents have become an Uncomplicated task, making it very difficult to understand between original and the artificial. So, it is a very big challenge for providing Security and verification of digital data. This paper put forward an idea or intimation to provide an innovative method to verify the digital documents. An advanced method of QR code is bring here, which allow us to embed digital data such as image in QR code. In this paper, we bring up a new technique, where the image is encoded in QR i.e. [Quick Response] Code in encrypted form, so that if a hacker tries to modify or tries to tamper with the data the data then he will be unsuccessful to do that. This is due to; the encryption key is unknown to him except from the authorized person. It is impossible to scan or have access to the encrypted QR code as QR codes are robust.*

Key Words: QR code, AES(Advanced Encryption Standard) Algorithm, Android platform,Digtal image, Secret key,Watermarking,Decryption

Problem Statement: After new technology of digitizing information were developed,a huge amount 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 not only for authorize access but for illegal access also.Much 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 ancient times as a cryptography and stegnography.

1. INTRODUCTION

A digital watermark is a kind of marker secretly embedded in a noise-permit signal such as an image data. It is typically used to identify proprietorship of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal the hidden information should, but doesn't need to, contain a relation to the carrier signal. Digital watermarks may be used to prove the authenticity or integrity of the carrier signal or to show the identity of its proprietor. The information to be embedded in a signal is called a digital watermark, although in some condition the term digital watermark means the dissimilarity between the watermarked signal and the cover signal. The signal where the watermark is to be embedded is called the host signal. A watermarking system is usually divided into three prominent steps, embedding, attack, and perception. In embedding, an algorithm obtain the host and the data to be submerged, and produces a watermarked signal. this paper contain QR code and steganography is used to furnish the security to important data.

1.1 QR Code

QR codes are 2 dimensional matrix. It allows to store a large volume of unique data. Bar-codes are one dimensional vector. So compare to bar-codes QR codes are having more storage size. QR codes can hold up to 7,089 numeric characters and up to 4,296 alphanumerical letter values as an information. The following figure shows the structure of a QR code.

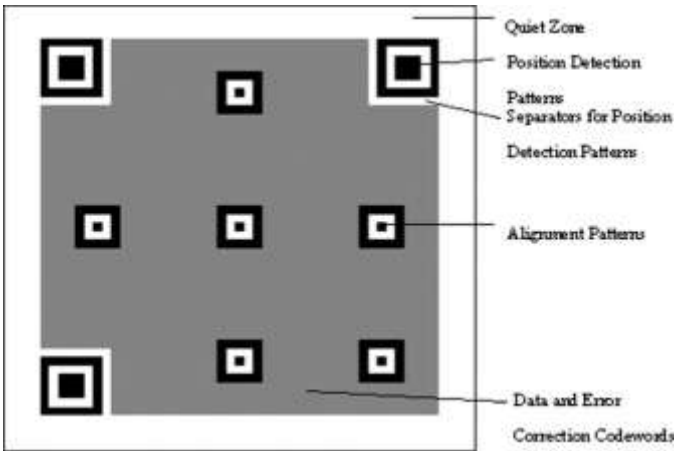

Fig-1: QR Code

1.2 Steganography

Steganography is an embedding process to hide the data in the form of an image or text. now a days sense of the word

sometimes refers to data or a file that has been hide within a digital image. What Steganography basically does is utilize human perception; the human senses are unqualified to look for files that have data hidden inside them. Generally, in steganography, the specific data isn't maintained in its original format and thereby it's converted into an alternate identical transmission file like image that successively is being hidden among another object. This apparent message (known as cover text in usual terms) is sent through the network to the recipient, wherever the specific message is separated from it. Steganography are used to achieve data privacy over confidentiality.

2. LITERATURE SURVEY

1. Image steganography with using QR code and cryptography: In this there is image stenography method that's enables us to to embed the encoded secret message using Quick Response Code (QR) code into the image information. Advanced Encryption Standard [AES] domain is introduced for the encryption of the QR code, whereas encrypting method is in addition secured by Advanced Encryption Standard (AES) cipher algorithmic rule. Also, typical characteristics of QR code was cracked using the encryption, therefore it makes the method more secure. The relation between security and capability of the strategy was improved by special confining of QR code before the embedding method.

2. Information Hiding using Image Embedding in QR Codes for Color Images: It is considered that embedding strategies are designed to be

Consistent with standard decoding applications and might be Enforced to any color or gray scale image with full space Coverage. The embedding technique consists of 2 main following components. First element is that the use of halftoning techniques for the choice Of varying the pixels to interrupt and decrease the coarse square Architecture of the QR code and second is that the brightness Level to that the pixels square measure to be re-created. In such some way that it shouldn't be visible to naked eye on the Color image. Afterwards decoding should be done for QR code from the color image With minimum errors.

3. Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System: In this paper, there's totally different methodology, where the QR code is embedded into the Image which act as a digital media. Then the message which the user wants to send to the receiver is inserted in that QR code which is hidden behind the image. After secret key or encryption key will be entered, so that if an intruder tries to modify the message then he cannot do this , as well as there is an image in front and behind the image there is QR code in which message is hidden In this project, message is double secure as if any one try to see the message they cannot this is because of the image in front of QR code advantage of this is the image cannot be scanned . In this Method encryption of the message is done using AES Advanced encryption standard encryption algorithm. The encrypted message are Entered inside QR code and that QR code is also hidden behind the image . The message can then be Accessed from the QR code and can be decrypted using Decryption algorithm Reverse of AES. then the message will be accessed using the secret key which is known to recipient.

3.SYSTEM ARCHITECHTURE

System architecture is the theoretical design that defines the structure and behavior of a system. An design explanation is a prescribed description of a system, systematized in a way that supports perceptive about the fundamental properties of the system. It outlines the system modules or building blocks and delivers a plan from which products can be secured, and systems developed, that will work organized to implement the whole system. The System architecture is shown below.

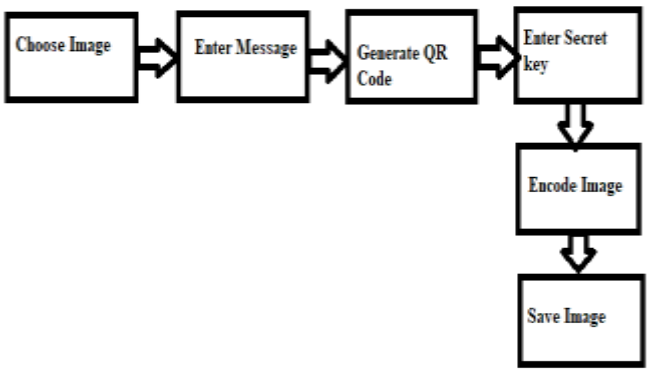

Fig -2: Encryption

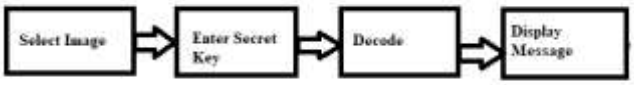

Fig -3: Decryption

4. CLASSIFICATION OF DIGITAL WATERMARKING TECHNIQUES

A] Robustness

Robustness is crucial property for all watermarking systems. There are so many ways by which watermark is degraded, altered during transmission, striked by hackers in paid media applications. So watermark should robust, So that it will resist against all the attacks and threats.

B] Effectiveness:

It is the most important property of watermark that the watermark should be effective means it should surely be detective. If this will not be happened then the goal of the watermarking is not fulfilled.

C] Host signal Quality:

It is also important property of watermarking. Everyone knows that in watermarking, watermark is embedded in host signal (image, video, audio etc.). This may have an effect on the host signal. So the watermarking system should be like that, it will least change the host signal and it should be unobtrusive when watermark is invisible.

D] Watermark Size:

Watermark is often use to owner identification or security approval of host signal and it always use when data is transmitted. So it is important that the size of the watermark should be less because it will increase the size of data to be transmitted.

E] Perception:

A digital watermark includes perception Presence in the marked signal is visible On videos and Images, some are made transparent/translucent for Convenience for consumers due to the fact that they block Portion of the view; therefore degrading it.

F] Capacity:

It can be described as number of data bits a Watermark gets encoded within a unit of time or work. Watermark Should be able to carry enough information that can Represent the uniqueness of image.

5. ALGORITHM

The AES algorithm gains vast application in our daily life, such as smart cards, cell phones, automated teller machines and WWW servers. AES encodes a plain text to become a cipher 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 clue to the original plain text.

All the computations in AES are implemented on bytes instead of bits. Therefore, 128 bits of plain text is treated as 16 bytes. These 16 bytes are located in a matrix of four rows and four columns. In AES 10 rounds are performed for 128 bit keys, 12 rounds for 192 bit keys, and 14 rounds for 256 bit keys. All of these rounds apply a different 128 bit key, calculated from the original AES key.15 Following is the Algorithm to encrypt the data:-

• Step 1:- Input a plain text of 128 bits of block cipher which will be arranged as 16 bytes.

• Step 2: - Add Round Key: - each byte is integrated with a block of the round key using bitwise XOR.

• Step 3:- Byte Substitution: - the 16 input bytes are substituted by examining S- box. The result will be a 4x4 matrix.

• Step 4:- Shiftrow: - Every row of 4x4 matrixes will be shifted to left. Entries which will be on the left side now will be on the right side.

• Step 5:- Mix Columns: - Every column of four bytes will be transformed by applying a distinctive mathematical function (Galois Field).

• Step 6:- Add Round Key: - The 16 bytes of matrix will be scrutinized as 128 bits and will be XORed to 128 bits of the round key.

• Step 7:- This 128 bits will be taken as 16 bytes and similar rounds will be performed.

• Step 8:- At the 10th round which will be last round a ciphered text will be produced.

Initially, the plain text of 128 bits of block cipher will be input, which will be treated as 16 bytes. Then, each byte will be non-discriminated with a block of the round key using bitwise XOR. From S-Box the 16 input bytes will be exchanged resulting 4x4 matrices.All rows of this matrix will be shifted to left. Shifting will be done as follows:-

1) First row will be not shifted.

2) Second row will be moved one position left.

3) Third row will be switched two positions to the left.

4) Fourth row will be shifted three positions to the left 16

As a result new matrices will be produced containing same 16 bytes but shifted with respect to each other. In MixColumn, every column of the matrix will be transformed by applying mathematical function such as Galois Field. The 16 bytes of matrix will be considered as 128 bits and will be XORed to 128 bits of round key.

6. APPLICATIONS

Digital watermarking may be used for a variety of Applications like :

1. Copyright protection.
2. Source tracking (different recipients get differently Watermarked content).
3. Broadcast monitoring (television news often contains
4. Watermarked video from international agencies).
5. Video authentication.
6. Content management on social networks.

7. CONCLUSION

In this method we have implemented a advanced solution to protect the asset of the user or owner by providing security by using method Digital Watermarking technique whose work is to protect the authenticity,copyright protection of owner using a strong media QR code.In addition to, the QR code is also hidden behind the image so that seeing at it the person will not be able to recognize that it contains QR code. We also classified the watermarking algorithms based On spatial and transform domain. Watermarking, which Belong to the data hiding field, has seen a lot of Research interest recently. There is a lot of work begin Conducted in different branches in this field. We classify the Techniques based on different areas in which data is Embedded. AES (Advanced Encryption Standard) provides more security (it is less susceptible to cryptanalysis than 3DES).

REFERENCES

[1] Image Steganography and Data hiding in QR Code Rutuja Kakade1, Nikita Kasar2, Shruti Kulkarni3, Shubham Kumbalpuri4, Sonali Patil5 Student, Dept of Computer Engineering, PCCOE, Maharashtra, India Associate Professor, Dept of Computer Engineering, PCCOE, Maharashtra, India

[2] V.Hajduk , M.Broda , O.Kováþ and D.Levický, "Image steganography with using QR code and cryptography," 26th Conference Radioelektronika, IEEE pp. 978-1-5090-1674-7, 2016

[3] A. Gaikwad and K.R.Singh, "Information Hiding using Image Embedding in QR Codes for Color Images: A Review," International Journal of Computer Science and Information Technologies, Vol. 6 (1) , 2015

[4] M. Broda, V. Hajduk, D. Levický, "Image steganography based on combination of YCbCr color model and DWT," in ELMAR, 2015 57th International Symposium, pp. 201- 204, 28-30, 2015.

[5] S. Dey, A.Nath and S. Agarwal, "Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System," International Conference on Com Improvement in the Performance and Security of Advanced Encryption Standard Using AES Algorithm and Comparison with Blowfish Amit Verma, Simarpreet Kaur, Bharti Chhabra, M. Tech. Research Scholar, Computer Science & Engineering, Chandigarh Engineering College 3Assistant Professor, Computer Science& Engineering, Chandigarh Engineering College, Landran, Punjab, India, Professor and Head of Department, Computer Science& Engineering,Chandigar Engineering College,Landran,Punjab.

[6] A Survey of Digital Watermarking Techniques and its Applications, Lalit Kumar Saini1, Vishal Shrivastava, M.Tech Research Scholar, Professor Department of Computer Science and Engineering, Arya College of Engineering. & Information Technology, Jaipur, India.

[7] "Digital Image Security Using Digital Watermarking " Prof.A.S.Kapse, Sharayu Belokar, Yogita Gorde, Radha Rane, Shrutika Yewtkar, Professor. A.S.Kapse, Dept. Computer Science & Engineering, P.R. Pote College of Engineering & Tech, Amravati, Maharashtra, India. BE student, Dept. of Computer Science & Engineering, P.R. Pote College of Engineering & Tech, Amravati, Maharashtra, India.

[8] Improvement in the Performance and Security of Advanced Encryption Standard Using AES Algorithm and Comparison with Blowfish Amit Verma, Simarpreet Kaur, Bharti Chhabra M. Tech. Research Scholar, Computer Science & Engineering, Chandigarh Engineering College Assistant Professor, Computer Science& Engineering, Chandigarh Engineering College, Landran, Punjab, India Professor and Head of Department, Computer Science& Engineering, Chandigarh Engineering College, Landran,Punjab,

[9] Chi-Feng Lu , Fast implementation of AES cryptographic algorithms in smart cards; Yan-Shun Kao; Hsia-Ling Chiang; Chung-Huang Yang; Security Technology, 2003.

[10] FIPS PUB 197, Advanced Encryption Standard (AES), National Institute of standards and Technology.