ISSN:0975-9646

Secure Message Transmission Ensuring Authentication Using Digital Signature and Watermarking

Shivi Garg[#1], Manoj Kumar[#2]

[#]*Computer Engineering Department,*
Delhi Technological University
Delhi, India

Abstract— **This paper presents a system that allows the users to securely transfer the messages by embedding them in the digital images. The information, which is to be sent to the receiver, is made to be more secure in spite of simple plain text. The message is hashed and digitally signed to provide authentication. The Quick Response (QR) Code for this secured information is generated. This QR Code image is accommodated in the original cover image by the embedding algorithm. This system uses the watermarking scheme. To accommodate the messages the original cover image is modified by the embedding algorithm to obtain the stego image. At the receiving end, the message is decoded using the other key value pair. The proposed system is not hacked by any intended user thereby ensuring authentication and non-repudiation.**

Keywords— **Digital Signature, Hash, QR code, Watermarking.**

I. Introduction

Many methods exist to make the information secure. Information security is the method of protecting information which protects its availability, privacy and integrity [1]. For providing secure message transmission cryptography is used in both wireless and wired network.

Cryptography is the study of techniques and methods for secure communication in the presence of third parties known as adversaries. Cryptography is a process of converting a plain text into cipher text (Encryption) and cipher text into a plain text (Decryption) [2]. Cryptography is mainly of two types: Symmetric key cryptography (or secret key cryptography) and Asymmetric key cryptography (or Public key cryptography). Secret-key cryptography is encryption method or a technique where both the sender and receiver share the same key. The sender uses an encryption algorithm and the key to encrypt the data; the receiver uses the corresponding decryption algorithm and this same key to decrypt the data. Public-key cryptography uses different set of keys for encryption (Public key) and decryption (Private Key).

In computer science and cryptography there is a type of function known as Hash function that plays a very important role in making messages secure. The predicate hash function is easy to compute whereas it is hard to invert, i.e., for a given output it is hard to find an input that maps to that output [3]. After the message is hashed, key pairs are generated to form digital signature. The encrypted hash is then embedded in the QR Codes, which is then hidden behind the cover image to form the watermarked image.

II. Digital Certificate Generation

A. Key Pair Generation

The key-pair generation is based on RSA Algorithm. RSA is a public key cryptosystem having two keys: public key and the private key [4]. Here, encryption is done using the private key and decryption is done using the public key. An RSA public-private key pairs can be generated by the steps mentioned as follow:

1. Generate a pair of large, random prime numbers: p and q.

2. Compute the modulus n such that $n = p * q$.

3. Compute $\varphi(n) = (p-1) * (q-1)$.

4. Chose ‘e’ such that $1 < e < \varphi(n)$ and e & n are co-primes.

5. Compute a value for ‘d’ such that $(d*e) \% \varphi(n) = 1$.

6. The public key is the number (e, n) & private key is (d, n).

To encrypt a message, M, with the public key, creates the cipher, C, using the equation: $C = M^e \bmod n$.

The receiver then decrypts the cipher, C, with the private key using the equation: $M = C^d \bmod n$.

B. Digital Signature Algorithm

A digital signature is a mathematical and computational scheme for representing the authenticity of a digital information or document. It ensures non-repudiation i.e., the sender of the message cannot later on deny having sent the message and that the receiver cannot deny having received the message and that maintains the integrity of the message i.e. it is not altered in transit [5].

A digital signature scheme generally consists of three algorithms:

1) A key generation algorithm, which chooses a private key uniformly at random from a set of possible private keys. This algorithm then produces the private key and a corresponding public key

2) A signing algorithm when, given a message and a private key, produces a signature

3) A signature verifying algorithm, which when given a message, public key and a signature, either accepts or discards the message's claim to authenticity

III. Proposed System

This system helps to merge the concepts of cryptography and watermarking. In this system payload is being inserted in the QR Code image which consists of the hash value of patient information. The payload is encrypted using a key (provided by the user) based on the digital signature algorithm before embedding. This digitally signed information is encoded into QR Code. This secure code is then embedded in an image to form the watermarked image. In case where the number of pixel pairs free for inserting the watermark outnumbers the length of the payload, then payload is repeated several times according to the requirement.

IV. Methodology

C. Embedding Process

1) The In this process patient information like-Name, Age and Sex are stored in the text file patient.txt.
2) Compute the hash of the patient information.
3) This hash is encrypted with the private key of the sender and digital signature is then generated. The key generation is based on RSA Algorithm. RSA is a public key crypto-system having two keys-Public Key and the Private Key.
4) The digitally signed information is encoded into the QR Code.
5) The secured code is then embedded in an image to form the watermarked image.

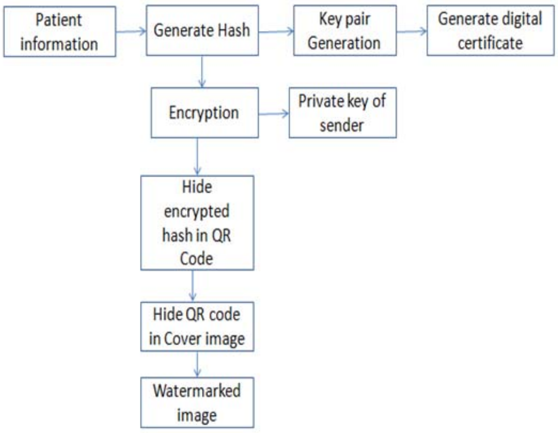


Fig. 1 Flowchart of Embedding Process

D. Restoration Process

1) In the restoration process we apply the extraction process of Coltuc et al. scheme and extract the encrypted QR Code.
2) To decode the QR Code any QR code decoder can be used and encrypted hash of the patient information is obtained.
3) To recover the original patient information it is decrypted by using the public key and the digital signature.
4) If some different QR code is decrypted, then this information will not match and it is rejected.
5) Or if the hash is not matched, then also it will be rejected confirming that the sender is not authentic and the image has been tampered.

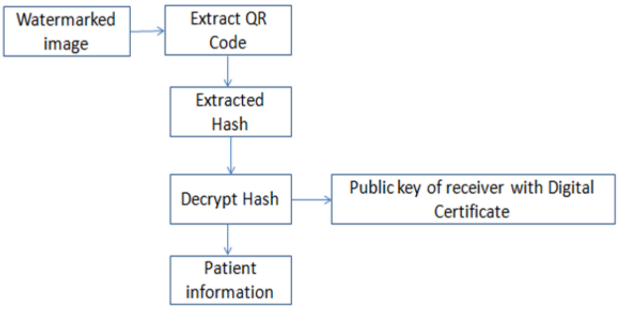
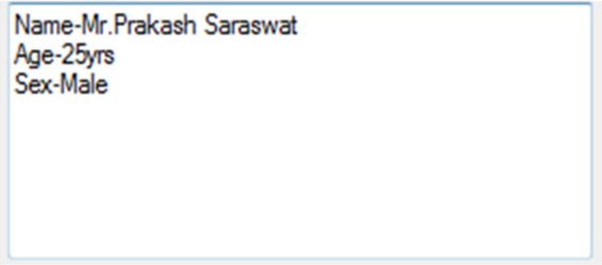


Fig. 2 Flowchart of Restoration Process

V. Results and Analysis

A. Patient Information

Patient information is a simple text file as patient.txt which contains the attributes like-Name, Age and Sex of the patient. Fig. 3 shows the patient.txt file.

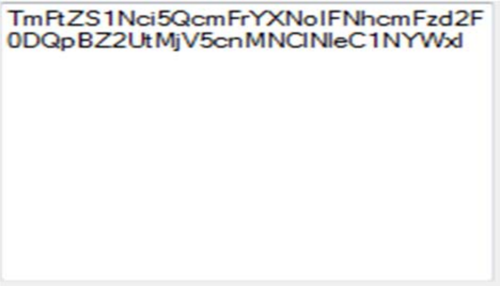


Name-Mr.Prakash Saraswat
Age-25yrs
Sex-Male

Fig. 3 Patient information in patient.txt file

B. Hash Generation

Hash of the patient information is generated using MD-5 (Message Digest). It produces 128 bit hash value and normally expressed in text format as a 32 digit hexadecimal number format [6]. Fig. 4 shows the hash of the patient information.

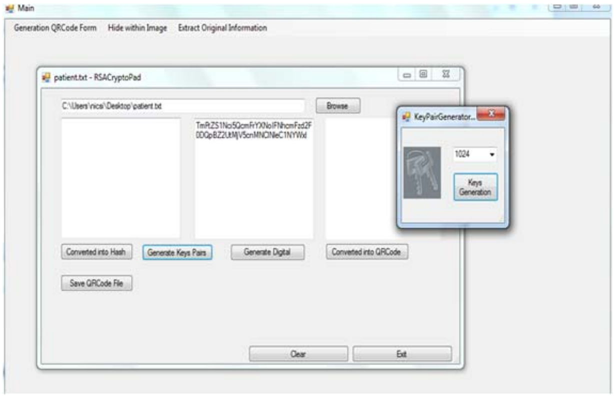


TmFtZS1Nci5QcmFrYXNoIFNhcmFzd2F
0DQpBZ2UtMjV5cnMNClNleC1NYWxl

Fig. 4 Hash of patient information

C. *Key Pair Generation*

Key pair generation is based on RSA algorithm. It is a public key cryptosystem which has two set of keys: private key and public key. Encryption is done using private key and decryption is done by public key [7]. Key pair generation is shown in the Fig. 5.



C:\Users\nicsi\Desktop\patient.txt

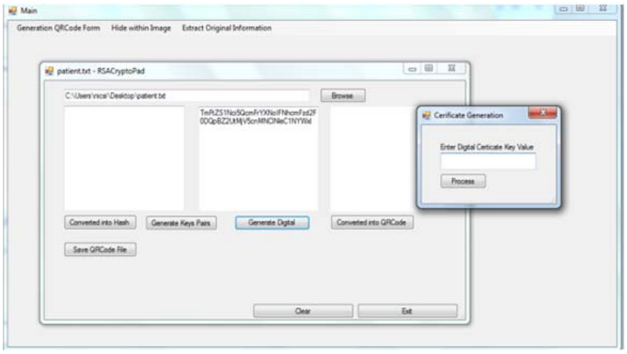
TmFtZS1Nci5QcmFrYXNoIFNhcmFzd2F 0DQpBZ2UtMjV5cnMNCiNleC1NYWxl

1024

Fig. 5 Key pair (public and private key) generation

D. *Digital Certificate Generation*

Digital certificates (also known as Public key Certificate) connect the identity of an individual or an institution to a digital public key, i.e., to a pair of keys that can be used to encrypt and sign digital information. The arrangement of principles, protocol standards and software that assist digital certificates is known as a public key infrastructure, or PKI. The software, which supports this infrastructure, generates a set of public-private key pairs. [8]. Fig. 6 shows the digital certificate generation.



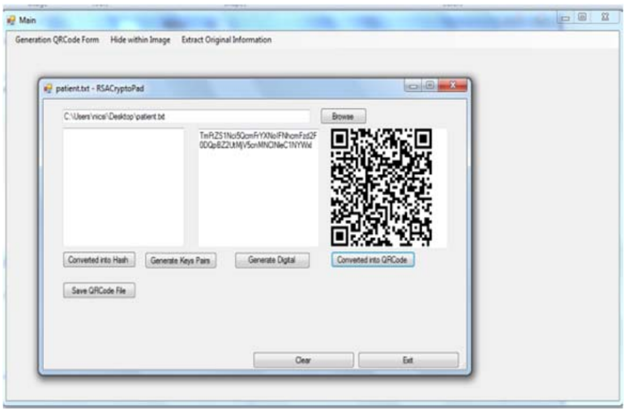
C:\Users\nicsi\Desktop\patient.txt

TmFtZS1Nci5QcmFrYXNoIFNhcmFzd2F 0DQpBZ2UtMjV5cnMNCiNleC1NYWxl

Fig. 6 Digital certificate generation

E. *QR Code Generation*

QR code (Quick response) is a two dimensional information storage tool. The length of the stored information depends on: Data type/Mode, Version (ranging from 1 – 40) and Error Correction Levels (L, M, Q, and H) [9]. The hashed information is encrypted using the Private key, which is then encoded to QR Code as shown in the Fig. 7.



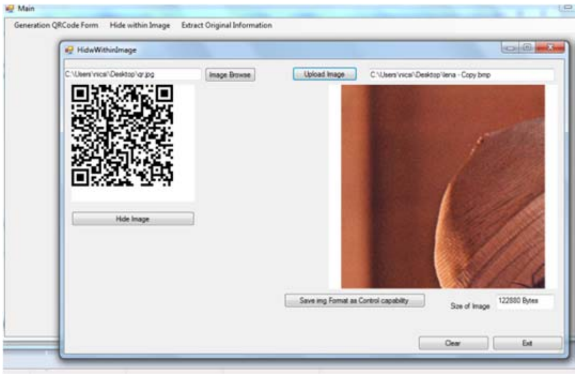
C:\Users\nicsi\Desktop\patient.txt

TmFtZS1Nci5QcmFrYXNoIFNhcmFzd2F 0DQpBZ2UtMjV5cnMNCiNleC1NYWxl

Fig. 7 Hash Encrypted with Private key and encoded to QR Code

F. *Watermark Generation*

The QR Code is then embedded in the cover image to generate the watermarked image. This is done by using Coltuc et al. scheme of reversible watermarking.[10]. Fig. 8 shows embedded QR code in the cover image to form watermarked image.



C:\Users\nicsi\Desktop\qr.jpg

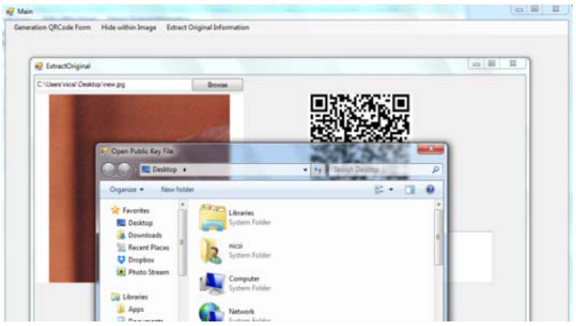
C:\Users\nicsi\Desktop\lena - Copy.bmp

Size of Image: 122880 Bytes

Fig. 8 QR Code hidden behind a cover image to get watermarked image

G. *Receivers' End*

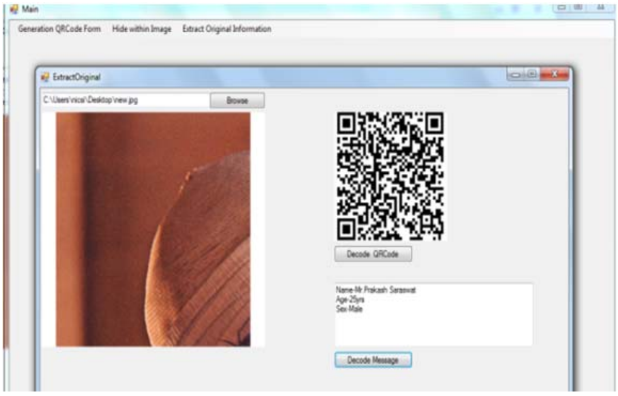
To extract the original information, public key of the receiver is used to decrypt the hashed information along with the digital certificate as shown in the Fig. 9.



C:\Users\nicsi\Desktop\new.jpg

Fig. 9 Decryption of hash using public key with digital certificate

If the key pairs match, then QR code is decoded to correct patient information as shown in the Fig. 10.

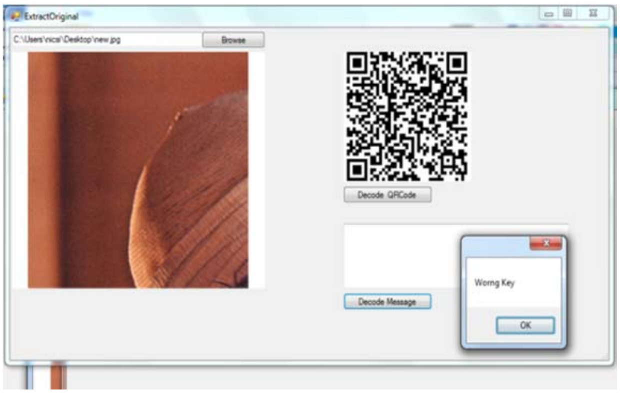


C:\Users\vica\Desktop\new.jpg

Name-Mr Prakash Saraswat
Age-25yrs
Sex-Male

Fig. 10 QR Code decoded to correct patient information

If the key pairs do not match, then QR code cannot be decrypted to the original information as in Fig. 11.



C:\Users\vica\Desktop\new.jpg

Worng Key

Fig. 11 QR Code decoded to wrong patient information

VI. CONCLUSIONS

The proposed scheme is robust to all the attacks. In this system the hash of the patient information is encrypted using the RSA encryption algorithm along with the generation of digital signature. This signed and encrypted hash is then embedded in the QR Code. This QR Code then embedded in the cover image using Coltuc et al. scheme. The embedding algorithm is made to work in feedback mode so that if a single bit of data gets changed, then following data gets changed too. And in that case the recovered hash and the hash of the recovered image will never match resulting in a rejected image.

ACKNOWLEDGMENT

It is a pleasure to acknowledge Dr. O.P. Verma (HOD computer engineering department) for the conversations and ideas that led to this research on secure message transmission. We would like to thank Dr. Seba Susan and Mrs. Ritu Agarwal for their important advice, corrections, and valuable suggestions, and for devoting their precious time on our research.

REFERENCES

[1] Vishwa Gupta, Gajendra Singh and Ravindra Gupta, *Advance cryptography algorithm for improving data security*, vol. 2, issue 1, January 2012

[2] Sangeet Saha, Chandrajit pal, Rourab paul, Satyabrata Maity and Suman Sau, *Encryption using different techniques: a review,* vol. 2, no. 1, January-February-2013.

[3] Marc Stevens, *Attacks on Hash Functions and Applications*, 2012.

[4] Sonal Sharma, Jitendra Singh Yadav, Prashant Sharma *Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm* vol. 2, issue 1, August 2012.

[5] D. Shiva Rama Krishna, *Providing security to confidential information using digital signature,* vol. 3, issue 11, November 2015.

[6] Xiaoyun Wang and Hongbo Yu, *How to break MD5 and other hash functions*, pp. 19–35, 2005.

[7] Amare Anagaw Ayele1, Dr. Vuda Sreenivasarao, *A Modified RSA Encryption Technique Based on Multiple public keys*, vol. 1, issue 4, June 2013.

[8] Dr. Ali M. Al-Khouri., *The role of digital certificates in contemporary government systems: the case of UAE identity authority*, 2010.

[9] Peter Kieseberg, Sebastian Schrittwieser, Manuel Leithner, Martin Mulazzani, Edgar Weippl, Lindsay Munroe and Mayank Sinha, *Malicious pixels using QR Codes as attack vector*, 2012.

[10] Dino Coltuc, and Alain Treméau, Simple *reversible watermarking schemes*, January, 2005.