Image Authentication using RSA and Chaotic Map

Chitra Solanki
M Tech student
DIT University
INDIA

Madhu Sharma
Assistant Professor
DIT University
INDIA

ABSTRACT

Authentication is basically a way by which sender and recipient must prove their identities to each other. Image authentication verifies the originality of an image by detecting malicious manipulations. Reliable image authentication technology must be able to protect an image from time it was first produced until the final stage of use. In this paper we describe an effective technique for image authentication which can prevent malicious manipulations by using RSA and Baker's map. Chaos refers to a type of complex dynamical behavior that possesses some special features such as being extremely sensitive to small variations in initial conditions. Moreover this is certificateless-based scheme and allows people to verify the signature without the certificate. For this reason, we do not need the certificate authority to store and manage user's certificates.

In 2014, Chin-Chen Chang, Chin-Yu Sun, and Shih-Chang Chang has given a similar designed certificateless-based signature scheme based on RSA operations; however, their scheme is modified and improved by using it on image rather than text [2].

General Terms

Chaotic map, RSA, Digital Signature, Random number, MD5. SHA-1.

Keywords

UACI and NPCR, correlation coefficient, certificateless.

1. INTRODUCTION

Most initial computer applications had no, or very little security as computer data was considered to be useful, but not something to be protected. This continued for a number of years until the importance of data was truly realized when computer applications were developed to handle financial and personal data [1]. Authentication identifies the user of a computer system, and builds a trust with the recipients of a message.

With the increasing dependence on digital media and the continued use of Internet to share information over it, the security of data and message authentication has become the real challenge for today's researchers [4]. Fabrication can be caused if there is lack of authenticity. Nowadays the increase in multimedia message brought the focus from text based authentication to image based authentication. This transition is due to the conventional textual encryption and authentication methods did not consider the large amount of correlation between adjacent pixels of an image and thus we cannot prove it secure [11]. The whole concept of authentication is based on determining who an individual user is, before allowing the user to go ahead and perform actual transactions using the system. Authentication provides a required level of assurance for determining an identity. The whole idea of authentication is based on secrets. In our scheme we have used random number which is generated by chaotic map and it becomes the basis of our authentication.

1.1 Need of Security and types of attacks

As technology improved, the communication infrastructure became extremely mature, and newer applications began to be developed for various user demands and needs. Soon , people realized that the basic security measures were not quite enough to prevent from different types of attacks [12].

Table 1. Table Showing the types of Passive Attacks

Passive attacks	
Release of message contents	Traffic analysis
When the contents of a confidential message is released against our wish then we say that confidentiality of message is lost or it is known as the case of Interception	If we send confidential messages in code language to ensure its confidentiality then if many such messages are passing through passive attacker will get a clue regarding code this is known as traffic analysis.

Table 2. Table Showing the types of Active Attacks

Active Attacks		
Interruption (Masquerade)	Modification (Alteration)	Fabrication (Denial of Service)
Masquerade is caused when n unauthorized entity pretends to be another entity	Alteration of messages involve some change to the original message	This attack prevent legitimate user from accessing some services.

Let us assume that a person wants to send a check worth Rs 10000 to another person B. Normally,

- A will like to ensure that no one except B gets the money, and even if someone gets it, she/he does not come to know about the content of the check. This is the principle of confidentiality. Interception causes loss of message confidentiality. Release of message contents also causes loss of confidentiality as if the contents is released against the senders wishes to someone else then confidentiality of message is lost. We can prevent the release of message contents by encoding a message, so that only the desired parties understand the contents of the message, because only they know the code language. However, if many such messages are passing with some sort of pattern that provides the attacker some clues regarding the communication. The attacker will try to analyze the encoded messages to come up with likely patterns and get some idea about the ongoing conversation. This type of attack is Traffic analysis [1].

- A and B further wants that nobody else can change the content of check such as amount, date, signature, name of the payee, etc. This is the principle of Integrity. Loss of integrity causes modification. Alteration of messages or creation of false messages is one type of modification another type is Replay attack in which a user captures a sequence of events and resends them. For instance, suppose user A wants to transfer fund to user B and A might send an electronic message to bank and it might be possible that B could capture this message and send a second copy of the same to the bank again and A have no idea about this unauthorized behavior of B. Therefore, B would get benefit of fund transfer twice, once authorized and once unauthorized through replay attack. Masquerade is also caused when an unauthorized entity pretends to be another entity.
- B would like to be assured that the check has come from A, and not from someone else who posed as A or someone fake. This is the principle of authentication. Fabrication is possible in the absence of proper authentication mechanisms. Denial of services(DOS) attacks cause the loss of service to a resource rather than unauthorized access of data. These types of attacks effort by overfilling the potential of your network, host or application. The DOS attack prevents your rightful customers from gaining access to your application. The attack can simply overload an application or could cause your complete computer system to crash. There are multiple forms of DOS attacks and protecting from them is difficult. Some attacks overload services that are running but not needed. Turning off unnecessary services is part of the prevention. Adding filter statements to your routers and firewalls can stop some attacks.
- If after the transaction from A's account to B's account is successful and the money Rs 1000 is transferred, then it is possible that after sometime A will claim that he haven't signed the check, in this case A's signature is used to disallow A to refute this claim. This is the principle of Non-repudiation. It does not allow the sender of a message to refute the claim of not sending the message.

1.2 Key Escrow Problem with Digital Signatures and certificates

Digital signatures meet the need for authentication and integrity. This is a digital document issued by certificate authority that uniquely identifies the sender. A message is run through a hash function and so given a value: the message digest. This digest, the hash function and the plain text encrypted with the recipient's public key is sent to the recipient. The recipient decodes the message with their private key, and runs the message through the supplied hash function to that the message digest value remains unchanged or the message should not be tampered or changed. Very often, the message is also time stamped by a third party agency, which provides non-repudiation [5].

In a traditional digital signature system, the signer normally holds two keys, a private key and a public key. The private key can be used for signing important messages, and give the corresponding public key to the certificate authority and verifier. The certificate authority (CA) stores and manages every user's public key. Once the verifier receives a signature from a signer and wants to verify it, CA will give the corresponding certificate to the verifier which includes the signer's public key. Hence, the verifier can verify the certificate and the signer's public key immediately. It is secure and very convenient but places a heavy burden on CA because the CA has to store and manage many certificates. For this reason, Shamir proposed an ID-based public key system in 1985 [6]. The users are allowed to use their identity information as their public key, and a private key generation center (PKGC) can generate users' private key which corresponds to the users' identity information. Unfortunately, some researchers have started to suspect the royalty of PKC because people feel anxiety about the CA holding their private key and privacy information. This is called the "key escrow problem" in some of the literature [6]. To overcome this problem, researchers have started to focus on the issues of the certificateless-based signature scheme.

This paper focuses on a scheme based on RSA and chaotic map to show that a strong certificateless signature scheme not only keeps the original security properties of the signature, i.e., integrity, authentication and non-repudiation, but also can protect the signer even if the attacker has strong power. We have used chaotic map that is Baker's map, Chaos is a word we all know usually meaning a lack of order or predictability which will make our scheme more secure and safe.

1.3 Baker's map

In recent years, the chaos based cryptographic schemes have suggested some new and efficient ways to develop secure image authentication techniques. In this paper we have proposed a new approach for image authentication based on chaotic Baker's map in order to meet the requirement of secure image transfer. Chaos describes the behavior of a system that is highly sensitive to initial conditions. Chaotic systems are not predictable over a long period of time and are also associated with fractal structures. Understanding chaos will help us understand why some systems exhibit seemingly random behavior yet are still systems that are determined by their initial conditions [7]. The properties of chaotic systems are:

- ✓ Deterministic, this means that they have some determining mathematical equations ruling their behavior.
- ✓ Unpredictable and non-linear, this means they are sensitive to initial conditions. Even a very slight change in the starting point can lead to significant different outcomes.
- ✓ Appear to be random and disorderly but in actual fact they are not. Beneath the random behavior there is a sense of order and pattern. The highly

> unpredictable and random–look nature of chaotic output is the most attractive feature of deterministic chaotic system that may lead to various novel applications [8].

Baker's map is a chaotic map from the unit square into itself. It is named after a kneading operation that bakers apply to dough: the dough is cut in half, and the two halves are stacked on one another, and compressed. In physics, a chain of coupled baker's maps can be used to model deterministic diffusion. Now, to consider the two-dimensional baker map, refer to (1)

$$B(x_n ; y_n) = (c x_n ; 2 y_n) \quad 0 \le y \le 0.5$$

$$(1 + c(x_n - 1),\ 2 y_n - 1) \quad 0 < y \le 1 \qquad \textbf{(1)}$$

where, $0 < c \le 0.5$

2. PROPOSED ALGORITHM

In this section, we propose an algorithm. There are three participants in our scheme: key generator center (KGC), signer, and verifier [2]. Our scheme consists of following steps which is described as follows.

```
Step1.   Apply R.S.A scheme by taking two large number's p and q and N = p*q and then generate public key e and private key d. and I ← read image
Step2.   MD5 ← hash map of I     /* authenticate image */
Step3.   SHA-1 ← hash map of I
Step4.   while no not equal to 1
Step5.   x← two random numbers between 1 and 100
Step6.   alpha ← 1.9999
Step7.   beta ← 0.25
Step8.   nStop ← 400 /* number of iterations */
Step9.   for n = 1:nStop
             s ← sign of x(1) /*  calculate signum*/
             fx(1) ← alpha*x(1) - s
             fx(2)← beta*x(2) + s/2.0

         end for
Step10.  R← mean of fx
Step11.  Ss←inverse of R
Step12.  No←ss*R
Step13.  end while
Step14.  x_uid← random 9 numbers
Step15.  C←Re X x_uid
Step16.  SPRK←x_uid X UIDd
Step17.  R_s1←UIDr_s1 X x_uid2*r_s1
Step18.  Encrypt image using value of R
         For i ←1 to r /* rows */
             for j←1 to c /* columns */
.                for k←1 to n /* channels */
                     Eimage[i,j,k]←I(i,j,k)
                 X R_s1

                 end for k
             end for j
         end for i
Step19. Display encrypted image
Step20. Decrypt image
         for i ←1 to r /* rows */
             for j ← 1 to c /* columns */
.                for k ←1 to n /* channels */
                     Dimage[i,j,k]
                 ←Eimage(i,j,k) / R_s1

                 end for k
             end for j
         end for i
Step21. Ih← calculate hash code MD5 of Decrypted image
Step22. DIh← calculate hash code SHA-1 of Decrypted image
Step23.  If MD5 is equal to Ih then
             If SHA-1 is equal to DIh then
                     Display Hash matches
             else
                         Display No match
             end if
         else
                     Display No match
         end if
Step24. results← calculate NPCR and UACI on Original and Decrypted image
```

3. RELATED WORK

We propose a strong RSA-based and chaotic map based certificateless scheme to improve image authentication scheme. There are three participants in our scheme:

- key generator center (KGC)
- signer and
- verifier

Our proposed scheme can be divided into three phases: I) setup phase, II) Image reading phase III) signing phase and IV) verifying phase. The details are described as follows:

I) Setup Phase:

In this step we use RSA scheme [7]. The KGC randomly take two prime numbers p and q, and compute its product which is N = p*q. Then KGC can choose public key (e) that satisfy (gcd e, Φ(N)) = 1. Here, Φ(N) denotes Eular's totient function. After that, KGC can find one private key (d) from computing ed=1 mod Φ(N) and selects two cryptographic hash functions MD5 and SHA-1. Finally, KGC sets parameter d to be the master secret key (MSK) and parameters e, MD5, and SHA-1 to be the master public key (MPK). MD5 is simple and easy to implement while SHA-1 chances of collision are less as compared to MD5 because of larger sized message digest [4].

II) Image reading phase:

Read original image I by inputting it from the user and calculating other units from it in an matrix form.

III) Signing Phase:

In this phase signer chooses a random number R generated by BAKER'S MAP (the baker's map is a chaotic map from the unit square into itself) and then compute its inverse R^{-1} that satisfies $R.R^{-1} = 1$. After that, he or she uses, secret value x_{UID} and KGC's master public key e to compute $C=R^e.x_{UID}$ and sends his identity UID and C to KGC. When KGC receives UID and C, KGC will use its master private key d to sign the received UID and C. After that, KGC sends UID^d and C^d back to the signer. When the signer receives UID^d and C^d, he or she can compute $C^d.R^{-1}$ to get $x_{UID}{}^d$. Finally, the signer can compute $x_{UID}{}^d.UID^d = (x_{UID}.UID)^d$ and sets $(x_{UID}.UID)^d$ as the private key. At the same time, signer can directly set her/his identity UID as the public key. In this phase signer chooses a random number r, and uses r to compute $R_r = UID_r.x_{UID}{}^{2r}$. After that, the signer can compute H = h (Rr, UID, I), where UID is the public key of signer and I is the original image. Then, the signer computes and $u_1 = x_{UID}{}^{H+r}$ and $u_2 = ((x_{UID}.UID)^d\ )^{r-H}$ to generate the signature delta = (H, u1, u2) and send the original image with the signature to the verifier [3].

I) Verifying Phase:

When the verifier receives the original image I with signature delta, he or she can use signer's public key (UID) and KGC's master public key which is e to compute $Rr' = (u2)^e.(UID)^H$ (u1). Then, the verifier can use Rr', signer's public key UID and then decrypt the original Image I and generate H' = h (Rr', UID, I), and verifies whether H is equal to H' If they are equal then the original image I is equal to decrypted image and one can believe that the signature is correct [2].

If original image is equal to decrypted image then it is authenticated otherwise not.

3.1 Discription of Authentication through equations:

$$H' = h(R_r', UID, I) \tag{2}$$

Now, from verifying phase

$$(R_r)' = (u_2)^e (UID)^H (u_1) \tag{3}$$

Refer to (2) and (3)

$$H' = h[\{(u_2)^e.(UID)^H(u_1)\}, UID, I] \tag{4}$$

From signing phase

$$u_2 = ((x_{UID}.UID)^d)^{r-H} \tag{5}$$

Now, refer to (4) and (5)

$$H' = h[\{(((x_{UID}.UID)^d)^{r-H})^e.(UID)^H(u_1)\}, UID, I]$$

$$H' = h[\{((x_{UID})^{ed}(UID)^{ed})^{r-H}.(UID)^H(u_1)\}, UID, I]$$

$$H' = h[\{(x_{UID})^{r-H}(UID)^{r-H}.(UID)^H(u_1)\}, UID, I]$$

$$H' = h[\{(x_{UID})^{r-H}(UID)^{r-H+H}.(u_1)\}, UID, I] \tag{6}$$

Again from signing phase

$$u_1 = (x_{UID})^{r+H} \tag{7}$$

Now, refer to (6) and (7)

$$H' = h[\{(x_{UID})^{r-H}(UID)^r(x_{UID})^{r+H}\}, UID, I]$$

$$H' = h[\{(x_{UID})^{r-H+r+H}(UID)^r\}, UID, I]$$

$$H' = h\{(x_{UID})^{2r}(UID)^r, UID, I\} \tag{8}$$

From signing phase

$$R_r = (UID)^r(x_{UID})^{2r} \tag{9}$$

Now, refer to (8) and (9)

$$H' = h(R_r, UID, I)$$

$$H = h(R_r, UID, I)$$

$$H' = H$$

Original image I = Decrypted Image Dimage.

1. EXPERIMENTAL RESULTS

In our scheme we have used Chin-Chen Chang, Chin-Yu Sun, and Shih-Chang Chang concept and tried to implement it in an image the following are the results we have received for correlation coefficient and NPCR and UACI.

A. Correlation coefficient analysis:

Correlation coefficient is the arithmetic determination of the degree to which modify to the value of one variable guess modification to the value of another. The linear correlation coefficient is sometimes referred to as the pearson product moment correlation coefficient to honor Karl Pearson who invented it [10]**.**The quantity cc which is called as the linear correlation coefficient, measures the strength and the direction of a linear relationship between two variables like x and y. The following equation (10) shows the formula of correlation coefficient.

$$cc = \frac{n\sum xy - (\sum x)(\sum y)}{\sqrt{n(\sum x^2)(\sum x)^2\sqrt{n(\sum y^2) - (\sum y)^2}}} \tag{10}$$

Where n is number of pairs of data

Table 3. Correlation coefficient between Encrypted, Decrypted and original images.

Correlation Coefficient of Encrypted image and Original is	Correlation Coefficient of Decrypted image and Original is
0.012386	.99888

Table 4. Correlation coefficient between plain images and their corresponding cipher images.

		CR Between adjacent pixels		
		Red	**Green**	**Blue**
Horizontal	Plain Image	0.9199	0.99588	0.9001
	Cipher Image	0.3489	0.2998	0.2996
Vertical	Plain Image	0.9158	0.8876	0.8999
	Cipher Image	0.012	0.1222	0.1999

B. Attributes:

Table 5. Attributes.

Abbreviation	Full form
RSA	Ron Rivest, Adi Shamir and Len Adleman
MPK	Master Public Key
Gcd	Greatest Common Divisor
UID	User's Identity
KGC	Key Generation Center
MSK	Master Secret Key
MD5	Message Digest
SHA-1	Secure Hash Algorithm
E	Public Key
D	Private Key
I	Original Image
NPCR	Number of changing pixel rate
UACI	Unified average change intensity

C. NPCR and UACI:

The number of changing pixel rate (NPCR) and the unified averaged changed intensity (UACI) are two most common quantities used to evaluate the strength of image encryption algorithms/ciphers with respect to differential attacks. Conventionally, a high NPCR/UACI score is usually interpreted as a high resistance to differential attacks. However, it is not clear how high NPCR/UACI is such that the image cipher indeed has a high security level. In this paper, we approach this problem by establishing a mathematical model for ideally encrypted images and then derive expectations and variances of NPCR and UACI under this model. Further, these theoretical values are used to form statistical hypothesis NPCR and UACI tests. Critical values of tests are consequently derived and calculated both symbolically and numerically. As a result, the question of whether a given NPCR/UACI score is sufficiently high such that it is not discernible from ideally encrypted images is answered by comparing actual NPCR/UACI scores with corresponding critical values. Experimental results using the NPCR and UACI randomness tests show that many existing image encryption methods are actually not as good as they are purported, although some methods do pass these randomness tests [9].

Table 6. NPCR and UACI

Image	Dimension	NPCR of different colour components			UACI of different colour components		
		Red	**Green**	**Blue**	**Red**	**Green**	**Blue**
Lena	512×512	98.90	98.95	98.98	32.98	32.68	32.67
Baboon	200×200	98.73	98.64	98.50	32.75	32.78	32.83
Peppers	200×200	98.90	98.48	98.66	32.69	32.83	32.77

D. Differential attack

One minor change in the plain image causes large changes in the cipher image then differential analysis may become useless. NPCR and UACI become two widely used security analyses in the image encryption community for differential attacks. NPCR concentrates on the absolute number of pixels which changes value in differential attacks while the UACI focuses on the averaged difference between two paired cipher images [10].

Suppose cipher images before and after one pixel change in a plaintext image are c1 and c2 respectively. The pixel value at grid (i,j) in c1 and c2 are denoted as c1(i,j) and c2*(i,j)* and a bipolar array D is defined by Equations (11) and (12). Then the NPCR and UACI can be mathematically defined by following Equations:

$$\mathrm{D(i,j)} = \begin{cases} 0, c^{1}(i,j) = c^{2}(i,j) \\ 1, c^{1}(i,j) = c^{2}(i,j) \end{cases} \tag{11}$$

$$\mathrm{NPCR} = N(c^{1}, c^{2}) = \frac{\Sigma i, jD(i,j)}{T} \times 100\% \tag{12}$$

$$\mathrm{UACI} = U(c^{1}, c^{2}) = \frac{\Sigma i, j \left| c^{1}(i,j) = c^{2}(i,j) \right|}{F \times T} \times 100\% \tag{13}$$

2. CONCLUSION

This efficient RSA-based scheme has been found to not only improve the security level but also solve the certificate management problem. In this paper, we proposed an efficient RSA-based certificateless signature scheme to improve the security of Chin-Chen Chang, Chin-Yu Sun, and Shih-Chang Chang scheme. Our proposed scheme makes the RSA-based certificateless signature system more powerful and secure. At the same time, use of chaotic map makes it unpredictable. Furthermore, it is easy to implement. For all of these reasons, our scheme is more suitable for an efficient certificateless-based signature systems.

In future we would like to implement this scheme for more multimedia messages like on videos and three dimensional images. Moreover, we have used a random number which was generated by Baker's map and the map which we have used is a 2d map but in future we can use chaotic 3d map to make a new scheme which is much more secure and stiff for cryptanalyst.

3. ACKNOWLEDGMENTS

I am thankful to my supervisor Mrs. Madhu Sharma Assistant Professor of the Division of Computer Science and Engineering for her proper guidance and valuable suggestions throughout the course of this paper. If not for the above mentioned people, my paper would never have been completed in such a successfully manner. I once again extend my sincere thanks to all of them.

My thanks to the experts who have contributed towards development of the template.

4. REFERENCES

[1] Atul kahate, 2003, cryptography and network security.

[2] Chin-Chen Chang, Chin-Yu Sun, and Shih-Chang Chang,2014, A Strong RSA-based and Certificateless-based Signature Scheme.

[3] Chitra Solanki, Madhu Sharma, 2015,An Efficient RSA-based and chaos-based Authentication Scheme.

[4] Pragya Agarwal, Shilpi Gupta, Anu Mehra, 2013,Transmission and Authentication of Text Messages through Image Steganography.

[5] Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Peter G. Neumann, Ronald L. Rivest Jeffrey I. Schiller, Bruce Schneier,1997, The risks of key recovery key escrow problem and trusted third party encryption.

[6] R.L RIVEST, A.SHAMIR, L.ADLEMAN.,1978,A method for obtaining digital signatures and public key cryptosystem, Association of compting machinery(ACM).

[7] George Makris , Ioannis Antoniou, 2012, Cryptography with Chaos, Proceedings, 5th Chaotic Modeling and Simulation International Conference, Athens Greece.

[8] Alireza Jolfaei, Abdolrasoul Mirghadri, 2011 Image encryption using chaos and block cipher.

[9] Yue Wu, Joseph P. Noonan, and Sos Agaian, 2011, NCPR and UACI Randomness Tests for Image Encryption.

[10] Narendra K Pareek , Vinod Patidar, Krishan K Sud, 2011, A Symmetric Encryption Scheme for Color BMP Images.

[11] B.Srikanth, G.Padmaja, Dr. Syed Khasim, Dr. P.V.S Lakshmi, A.Harita, 2014, Secured Bank Authentication using Image Processing and Visual Cryptography.

[12] Tanmay Bhattacharya, Sirshendu Hore， S. R. Bhadra Chaudhuri, 2012, An Image Authentication Technique by Handwritten Signature Verification using DWT and ANN.