An efficient signcryption method using fractal image coding scheme

Nadia M. G. Al-Saidi

Abstract—The major aim of the computer and the commutation security research is to achieve secure and authenticated message delivery/storage. This can be satisfied using digital signature followed by encryption. The functionality combining of an encryption scheme with that of a signature scheme is called signcryption. An efficient signcryption scheme using the compression capability of fractal encoding and decoding scheme is proposed in this paper. In the proposed scheme the message is encrypted using an efficient encrypted method, and a secure digital signature is constructed using hash function. Using the advantages of fractal image coding (FIC), the fractal codes of a digital signature are added to the encrypted message to be transmitted. At the receiver side, the hash function is constructed for the received encrypted message, after decryption. By comparing the received hash with the calculated one the verification process is performed to identify the integrity of the message. The message is accepted only if the verification process is success, otherwise the message is ignored. The proposed scheme is analyzed and discussed from the attacker viewpoint to prove that the scheme provides essential security requirements. The properties and the software implementation for the proposed scheme are discussed in details.

Keywords—Digital signature, Signcryption, Fractal image coding (FIC), Hash function, Attractor, RSA public key.

I. Introduction

INFORMATION security is concern with providing assurances about data. It is classified as the provision of the following services: confidentiality (the assurance that data is not disclosed to unauthorized parties), integrity (the assurance that data is genuine), and availability (the assurance that data is readily accessible). It must provide techniques capable of supplying confidentiality, integrity, and availability for society that can benefit from the advantages offered by electronic data storage and open networks [1]. Communication over open networks represent easy picking for an adversary who wants to intercept, modify, or inject data; similar threats are forced the data stored on networked computers. However, there are increased demands for digital signature to ensure the integrity and authenticity of digital information's and documents.

Many digital signature algorithms (DSAs) has been developed since Diffie and Hellman [2] seminal paper on public key cryptosystems was presented in 1976 [3]. Most current digital signature schemes are based on mathematical algorithm that required very complex mathematical computations. The sender is digitally signing a document by using a computer, while the receiver verifies the validity of the signature also by using the computer. Building a digital signature scheme with high security and without complex mathematical computations is big challenge until now [4].

In order to establish a confidential channel between two users in a large networks such as internet, modern public key cryptography is required to provides a mechanism in which the key to be exchange do not need to be secret. It has revolutionized the way for people to conduct secure and authenticated communications. Achieving authenticity of public keys can be done by two step approach, signature then encryption. These two steps consume machine cycles and also introduce "expanded" bits to an original message, whereas the cost for delivering a message is essentially the sum of the cost for digital signature and that for encryption. The question now; "*is it possible to transfer a message of arbitrary length in a secure and authenticated way with an expansive less than that required by signature then encryption?* The answer to this question is a new cryptographic primitive termed as "*signcryption*", introduced in 1997 by Zheng [5], which simultaneously fulfills both the function of digital signature and public key encryption in a logically single step and with smaller cost.

Given the complicated mathematical structure and deterministic nature, especially their recursive construction, fractal functions have many uses in applied sciences [6]. The latest application of certain elements of fractal geometry, namely the aforementioned fractal function, is in the cryptographic systems. It has the potential of creating new ways for securing important information to be transmitted or stored [7]. Fractal image coding has been extensively used in image recognition, image compression, computer graphics, etc. Most fractal image techniques utilize the block based fractal code as a representation or mapping function. The fractal code of an image may be considered as a compressed representation of the self similarity of the image blocks [8]. Due to several advantages of using fractal function. There are many proposals for incorporating fractal and chaos functions into the design of cryptographic and steganographic techniques.

This paper is organized as follows. The basic of fractal theory is briefly outlined in Section 2. In Section 3, an overview of materials and methods used are presented. Section 4 is devoted to some preliminaries on signcryption and its

Nadia M.G. Al-Saidi is with Applied Sciences Department-Applied Mathematics University of Technology -Baghdad-Iraq. Tel : +9647901305365/ e-mail: nadiamg08@gmail.com

desired attributes. The proposed algorithms with the software implementation are described in Section 5. Section 6, outlined the analysis and discussion for the proposed methods followed by a brief conclusion in Section 7.

II. The Fractal Theory

A. Fractal and the Iterated Function System

The fractals theory is a new discipline that offers a new method to research the self-similarity objects and irregular phenomena. It is an active branch of nonlinear science starting from the 1970s. Fractal has proven to be suitable in many fields and particularly interesting in various applications of image processing. Some phenomena which cannot be explained with Euclidean geometry could be interpreted with fractal geometry. Fractal theory and its methodology provide people a new view and new ideas to know the world, and it made our way of thinking enter into the nonlinear stage. First important advances are due to M. F. Barnsley [9], who introduced for the first time the term "Iterated Function Systems (IFS)" based on the self-similarity of fractal sets. Barnsley's work assumes that many objects can be closely approximated by self-similarity objects that might be generated by use of IFS simple transformations. From this assumption, the IFS can be seen as a relationship between the whole image and its parts, the main problem being how to find these transformations (the IFS) [10]. There is, in fact, a version of the IFS theory, the Local Iterated Function Systems theory that minimizes the problem by stating that the image parts do not need to resemble the whole image but it is sufficient for them to be similar to some other bigger parts in it. It was Arnaud E. Jacquin [11], who developed an algorithm to automate the way to find a set of transformations, providing good quality to the decoded images.

The main idea of fractal image coder is to determine a set of contractive IFS transformation to approximate each block of the image in order to generate the whole image. Some background for fractal theory to understand the IFS and FIC are given with more details in [12-14].

B. Fractal Image Coding

The goal of FIC is to be able to store an image as a set of IFS transformation instead of storing individual pixel data. The local iterated function systems are used because we work on a section of the image instead of the whole image. The process of encoding the image M requires us to find a collection of contractive maps $w_1, w_2, \ldots, w_n$ with $W=\bigcup w_i$ and M as the fixed point (attractor) of the map W. The fixed-point equation $M = W(M) = w_1(M) \cup w_2(M) \cup \ldots \cup w_n(M)$ suggests that we partition M into pieces to which we apply the transforms w_i to get back the original image M [15].

The metric space of a digital image is (μ, D_l), where D_l is the root mean square metric instead of the Hausdorff metric to compress the image $M \in \mu$. It is necessary to find $W: \mu \to \mu$, such that $D_l(M, W(M)) \cong 0$. This metric space is determined by partitioning the original image M into a set R of non-overlapping range blocks that cover M, and a set D of overlapping domain block that has twice the side of the range blocks and must intersect M as illustrated in Figure 1. The aim of FIC is to enable the collage theorem find the set of IFS transformation W for the image M whose attractor look likes M. This theorem allows also for the scaling factor in addition to rotations and reflections.

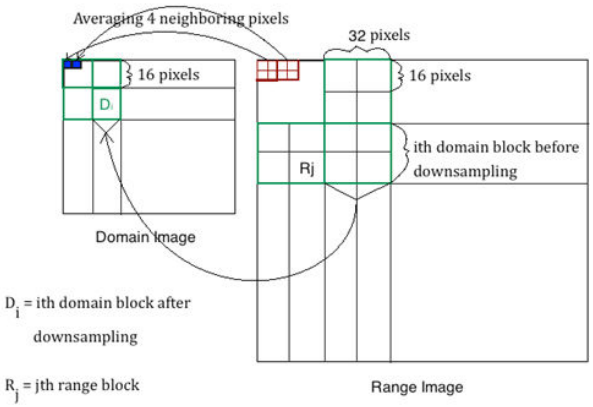


Figure 1: Generation of domain image from range

The question now, is how do we map domains to ranges? To find the corresponding domain block for each range block, we have to test all the domain blocks. After we find the optimized domain that minimize the D_l distance, the coordinate of domain pixels will be recorded in the compressed file.

Every pixel in the blocks is represented as a point P with the coordinates (X,Y,Z), where X and Y represent the standard geometric position of P. The gray level of P is represented by the Z-coordinate. To include the gray scale value 3-dimentional matrix is used. The transformations are specified by,

$$w_i \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} a_i & b_i & 0 \\ c_i & d_i & 0 \\ 0 & 0 & s_i \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} + \begin{bmatrix} e_i \\ f_i \\ o_i \end{bmatrix} \quad (1)$$

Where a,b,c,d,e, and f represent the scaling, rotation, reflection, and translation parameters, and the gray scale is controlled by $m(Z)=S.Z+O$, where S is the contrast and O is the brightness. The distance that we need to minimize is the distance between the gray scale levels. S and O can be computed using the least squares regression as in (2).

$$L = \sum_{i=1}^{n} (s \cdot a_i + o - b_i)^2 \quad (2)$$

Then the minimum of L occurs when the partial derivatives with respect to S and O are zero, which result in,

$$S = \frac{\left[n \sum_{i=1}^{n} a_i b_i - \sum_{i=1}^{n} a_i \sum_{i=1}^{n} b_i \right]}{\left[n \sum_{i=1}^{n} a_i^{\,2} - \left(\sum_{i=1}^{n} a_i \right)^2 \right]} \quad (3)$$

$$O = \frac{1}{n} \left[\sum_{i=1}^{n} b_i - s \sum_{i=1}^{n} a_i \right] \quad (4)$$

The D_l difference is calculated using (5) as follows,

$$L = \frac{1}{n}\left[\begin{array}{l} \sum_{i=1}^{n} b_i^{\,2} - s\left(s\sum_{i=1}^{n} a_i^{\,2} - 2\sum_{i=1}^{n} a_i b_i + 2o\sum_{i=1}^{n} a_i \right) + \\ o\left(no - 2\sum_{i=1}^{n} b_i \right) \end{array}\right] \quad (5)$$

Each range block is compared to all possible transformed domain blocks by calculating L to choose the one that minimizes L [14] . The decoding process is much simpler and (starting with an initial image M_0 usually a uniform grey or white image) can be achieved by iterating through the collection of maps. On the first iteration, $M_1 = W(M_0)$, and on the second iteration, $M_2 = W(M_1) = W(W(M_0))$, etc. This process can be repeated until the attractor resembles the original image. The Minimization process to choose the suitable range block for each domain block is graphed as in Figure 2.

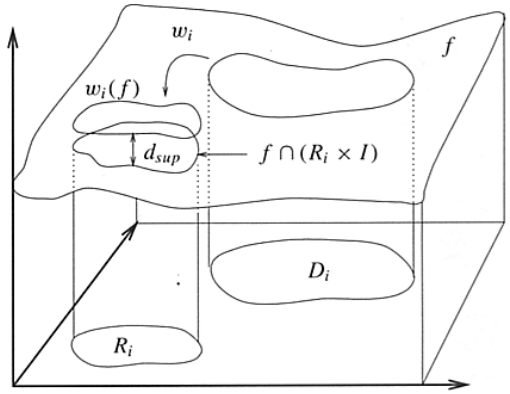


Figure 2. This figure is to minimize the difference between the part of the graph $F\cap(R_i \times I)$ above R_i and the image $w_i(f)$ of the part of the graph D_i

III. Material and Methods

The proposed method in [16] is based on the traditional methods that first find the digital signature scheme to demonstrating the authenticity of a digital message or document, and then encrypt the digital signature. In a aforementioned proposed scheme, RSA public key cryptosystem is used as an encryption method, whereas the signature is transacted between two communicating parties using a novel scheme based on FIC that have been illustrated in Section 2, to ensure a secure and authenticated transactions. In this paper a modification for this method is performed through using a new cryptographic primitive, called signcryption, which simultaneously fulfills both the function of digital signature and public key encryption in a logically single step, and with a cost significantly smaller than that required by signature then encryption [5]. The background material for the methods used in this proposal is overviewed as follows.

A. Public key system

RSA system is a public key algorithm, named after its inventors Rivest, Shamir, and Adleman. The security of the RSA system is based on the difficulty of factoring integer that is the product of two large prime numbers of approximately equal size. In a public-key encryption system each entity A has a public key e and a corresponding private key d. In secure systems, the task of computing d given e is computationally infeasible [17]. To describe the RSA digital signature scheme, note that the encryption function $E_k = Y(e, n)$ and the decryption function $D_k = Y(d, n)$ in the RSA system are commutative: that is,

$$D_k(E_k(x)) = E_k(D_k(x)) \equiv x^{ed} \equiv x \bmod n, \text{ for all } x \in Z_n.$$

Suppose that a user has a public key (e, n) and a private key (d, n). Then the private key is used to encrypt a message (or a file) $m \in Z_n$, where the signature is $S = D_k(m) = m^d \bmod n$. Anyone seeing the message m and the signature S can compute $m_1 = E_k(S)$ using the public key (e,n), and accept the signature if and only if $m_1 = m$.

B. Digital signature protocol

Achieving authenticity of public keys can be done in several ways. Public key cryptosystems are essential for electronic commerce or electronic banking transactions; they assure privacy as well as integrity of transaction between two parties. A Digital signature, Figure 3, is used to sign electronic documents and they are also mostly based on public key techniques [1]. It is a type of symmetric cryptography used to simulate the security properties of a handwritten signature on the paper. It is consist of three algorithms:

- a key generation algorithm,
- a signature algorithm, and
- a verification algorithm.

The authentication of a basic message is mainly provided by the digital signature. It can also provide non-repudiation, meaning that the authenticity of signed message can be verified publicly, not only by the intended recipient.

The reason for applying a digital signature in cryptosystems is to satisfy the,

(1) *Authentication:* Digital signatures can be used to authenticate the source of the messages. When the ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user.

(2) *Integrity:* The sender and the receiver of a message must be confident that the message is not subject to alteration during transmission.

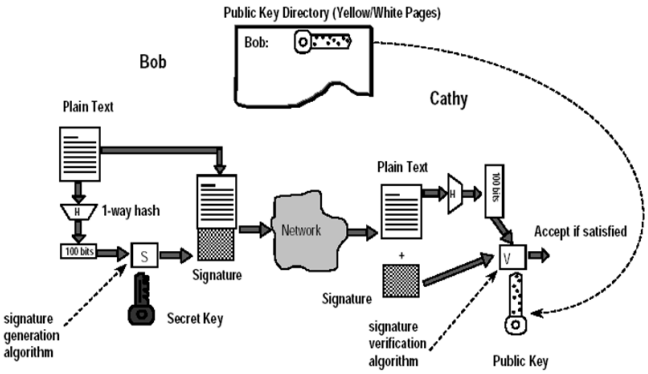


Figure 3: Digital signature mechanism

The problem with the public key based signature schemes is that, if the message is long, then the signature will take a long time to compute. To overcome this problem, hash functions that map a (possibly length) message to a small digest $h(M)$ are used [18].

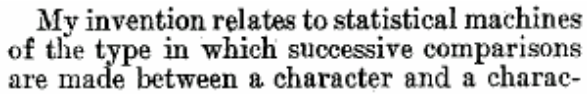
C. Hash Function

A one way function is a function that is easy to compute but hard or infeasible to invert. A cryptographic hash function, $h(M)$ takes an arbitrary length message as input and produces a fixed length output. The input is typically a file or a message. The output of the hash function is called Message Digest (MD) or hash value or message fingerprint. The most common cryptographic use of hash function is with digital signatures for data integrity. The inability to find two messages with the same hash-value is a security requirement, since otherwise the signature on one message hash value would be the same as that on another [19]. Hash function represented in many areas of the information systems (e.g. password identification, integrity control, database comparing, etc.). Its main purpose is to satisfied message integrity. It has the following properties: [18]

- The length of $h(M)$ should be small so that messages can be signed efficiently.
- The function h should be a publicly known one-way function – it should be hard to find a message that hashes to a pre-specified value.
- It should destroy algebraic relationships between messages and signatures.
- It should be collision-resistant, that is it should be difficult to find two messages with the same hash value, or more precisely: an attacker should not be able to find a pair of messages M≠ M' such that h(M)=h(M') with less than about $2^{t/2}$ work.
- Preimage-resistance: An attacker given a possible output value for the hash Y should not be able to find an input X so that Y = h(X) with less than about 2^t work
- Second preimage-resistance: An attacker given one message M should not be able to find a second message, M' to satisfy h(M) = h(M') with less than about 2^t work.

D. Optical Character Recognition (OCR)

It is software designed to electronically identify and translate printed or handwritten characters by means of an optical scanner. OCR is composed of three elements: scanning, recognition, and reading text. The OCR software scans and determines whether it is identifying images or text. Then, the machine determines letters and words by recognizing their shape by repetitions or patterns of familiar forms as in the following example [20].


My invention relates to statistical machines of the type in which successive comparisons are made between a character and a charac-

My invention relates to statistical machines
of the type in which successive comparisons
are made between a character and a charac-

IV. The Signcryption

Over the past two decades since public key cryptography was invented, signature then –encryption has been a standard method for one to deliver a secure and authenticated message of arbitrary length, and no one seems to have ever questioned whether it is absolutely necessary for one to use of the cost for signature and the cost for encryption to achieve both contents confidentiality and origin authenticity [5]. Until Zheng came to think about this question and answered it through introducing the concept of "signcryption".

Generalized Signcryption Definition: A Generalized signcryption scheme $\sum$=(Gen, SC, DSC) consists of three algorithms: Gen is a keys generation algorithm. SC is a probabilistic signcryption algorithm. It takes the private key of the sender S, and the public key of the receiver R, and a message $m \in M$ to return a signcryption text w. For any $m \in M$, $w \leftarrow SC(m, SDK_S, VEK_R)$. SDK is a secret key. VER ia a public key. When $R \in F$, $SC(m, SDK_S, VEK_R)=Sig(m, SDK_S)$, $DSC(w, SDK_R, VEK_S) =Ver(t, VEK_S)$. DSC is a deterministic unsigncryption algorithm. The public key of the sender S , the private key of the receiver R and a signcryption text w, is taken to return the message m or an invalid notation. For any signcryption text w, $m \cup \{\perp\} \leftarrow DSC(w, SDK_R, VEK_S)$. When $S \in F$, $SC(m, SDK_S, VEK_R) =Enc(m, VEK_R)$, $DSC(w, SDK_R, VEK_S)=Dec(e, SDK_R)$. Where, Enc= (Gen,Enc,Dec) is an encryption scheme: $e=Enc(m, VEK_R)$, $m=Dec(e, SDK_R)$. [21] Any signcryption scheme should have the following properties:

1. ***Correctness:*** A signcryption scheme $\sum$=(Gen, SC, DSC) is correct only if for any sender S, receiver R, and message $m \in M$, $\exists DSC(SC(m,SDK_S,VEK_R), SDK_R,VEK_S)=m$
2. ***Efficiency:*** The computational costs and communication overheads of a signcryption scheme should be smaller than those of the best known signature-then-encryption schemes with the same provided functionalities.

3. ***Security:*** A signcryption scheme should simultaneously fulfill the security attributes of an encryption scheme and those of a digital signature. Such additional properties mainly include: *Confidentiality, Unforgeability, Integrity*, and *Non-repudiation*. Some signcryption schemes provide further attributes such as *Public verifiability* and forward secrecy of message confidentiality while the others do not provide them.

Such properties are the attributes that are required in many applications while the others may not require them. Hereunder, the abovementioned attributes are briefly described.

- ***Confidentiality:*** It should be computationally infeasible for an adaptive attacker to gain any partial information on the contents of a signcrypt text, without knowledge of the sender's or designated recipient's private key.
- ***Unforgeability:*** It should be computationally infeasible for an adaptive attacker to masquerade an honest sender in creating an authentic signcrypt text that can be accepted by the unsigncryption algorithm.
- ***Non-repudiation:*** The recipient should have the ability to prove to a third party (e.g. a judge) that the sender has sent the signcrypt text. This ensures that the sender cannot deny his previously signcrypt texts.
- ***Integrity:*** The recipient should be able to verify that the received message is the original one that was sent by the sender.
- ***Public Verifiability:*** Any third party without any need for the private key of sender or recipient can verify that the signcrypt text is the valid signcryption of its corresponding message.
- ***Forward Secrecy of message confidentiality:*** If the long-term private key of the sender is compromised, no one should be able to extract the plaintext of previously signcrypt texts. In a regular signcryption scheme, when the long-term private key is compromised, all the previously issued signatures will not be trustworthy any more. Since the threat of key exposure is becoming more acute as the cryptographic computations are performed more frequently on poorly protected devices such as mobile phones, the forward secrecy seems an essential attribute in such systems.

The cost for signcryption is significantly smaller than that required by \signature followed by encryption". For typical security parameters for high level security applications (size of public modulo i = 1536 bits), signcryption costs 58% (50%, respectively) less in computation time and 85% (91%, respectively) less in message expansion than does \signature followed by encryption" based on the discrete logarithm problem (factorization problem, respectively) [22].

V. The Proposed Schemes

A. Signature Verification Algorithm

This algorithm is based on using fractal image coding scheme. The signature is digesting using the hash function SHA-1, and encrypted and verified using RSA digital signature. The algorithm consists of three parts.

1-Key generation

a- Given two large prime p,q, where $n=p*q$, and $\phi(n)=(p-1)(q-1)$

b- Select e such that $(e, \phi(n))=1$, find $d=e^{-1} \bmod \phi(n)$

c- The public key is (d,n), and the private key (e,n).

2-Signature

a- Determine the message M to be signed.

b- Calculate a one-way hash function HSs=SHA-1(M).

c- Encrypt HSs using the private key (d,n) such as, $Y=(HSs(M))^d \bmod n$.

d- Generate image IM that capture Y using text to image converter.

e- Apply fractal image coding scheme to find the set of the IFS coefficients, matrix T.

f- The signature is $S=T$

g- Send (S,M) to the receiver.

3-Verification

a- After receiving (S,M), the receiver use SHA-1 to find HS_v=SHA-1(M)

b- Generate the attractor IM1 from T using fractal decoding process.

c- Use OCR to read the encrypted hash Y in IM1.

d- Decrypt Y using the public key (e,n) to calculate HSs, such as, $HSs=Y^e \bmod n$

e- The signature is verified if $HSs=HS_v$,

B. Signcryption Algorithm

A new signcryption scheme based on RSA public key cryptosystem is proposed. This scheme used fractal image coding scheme to provide an authenticated transaction of the signcryption over an open and unsecure channel.

The RSA cryptosystem involves two parameters public to all users: They are n a large prime that is captured from the generated large primes p and q, such that $n=p.q$, and g is an integer in $\{1,\ldots,n-1\}$

For two communicated people the sender and the receiver the RSA parameters are as follows:

1- The key generation

a- The sender private key is an integer e_s: $0<e_S<\phi(n_s)$ where $\phi(n_S)=(p-1)(q-1)$, such that $\gcd(e,\phi(n_S))=1$.

b- The sender public key is $d_S=e^{-1} \bmod \phi(n_S)$ or $d_S=g^{e_S} \bmod \phi(n_S)$.

c- The receiver private key is an integer e_r: $0<e_R<\phi(n_R)$ where $\phi(n_R)=(p-1)(q-1)$, such that $\gcd(e,\phi(n_R))=1$.

d- The receiver public key is $d_R=e^{-1} \bmod \phi(n_R)$ or $d_R=g^{e_R} \bmod \phi(n_R)$.

For any sender to signcrypt a message m for the receiver, the following steps are carried out. The signcryption parameters are;

a- For the sender $\{e_S,d_S\}$.

b- For the receiver $\{e_R,d_R\}$.

c- E_k and D_k is the encryption and decryption algorithms.

2- The signcryption

a- Determine the massage M to be signcrypt.

b- Pick a random number $x_{\in R}\{1,\ldots,n_R\}$.
c- Calculate $k=(d_R)^x \bmod n_R$.
d- Find $r=\mathrm{HS}(m,k)$ where HS is the Hashing function.
e- Calculate $s=x/\{(r+e_S) \bmod n_S\}$.
f- Generate image IM that capture r and s using text to image converter.
g- Apply fractal image coding scheme to find the set of the IFS coefficients, matrix T.
h- Encrypt the message M to find $C=E_k(M)$.
i- Send the signcryption (T,C) to the receiver.

3- The unsigncryption

After receiving (T,C), the receiving performs,

a- Generate the attractor IM1 from T using fractal decoding process.
b- Use OCR to read the information in IM1.
c- Calculate the decryption key k such that,

$$k=(d_S.g^r)^{s.e_R} \bmod n_R.$$

d- Decrypt C to find the message $m=D_k(C)$.
e- Accept m as a valid message originated from the authorized sender only if $r=\mathrm{HS}(m,k)$

C. Software Implementation

The two algorithms with their graphic user interface (Figure 4 &5) are carried out using Java under Net-Beans IDE 7. The results have been obtained using a computer with the specifications; 2.4 GHz Intel COR i3 CPU and 4 GB RAM.

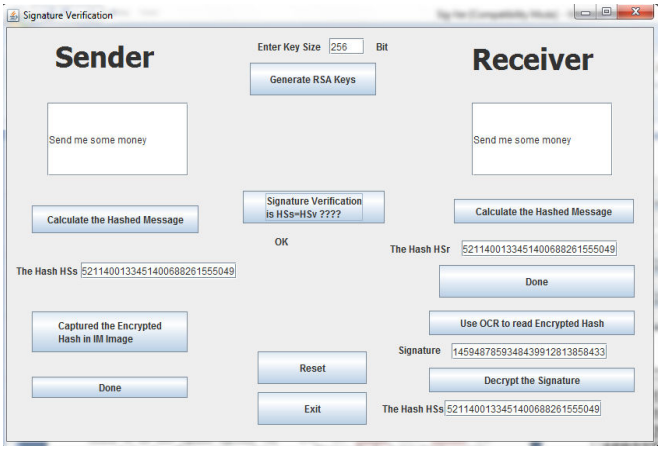


Figure 4. User Interface for Signature Verification using Fractal Image Coding software

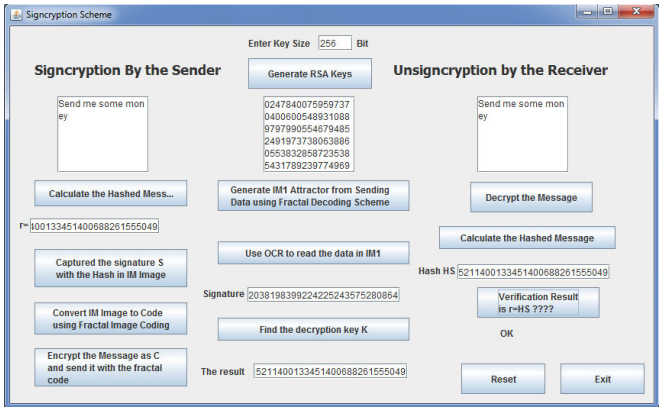
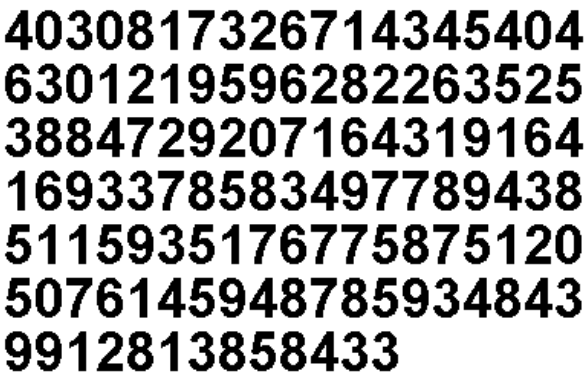


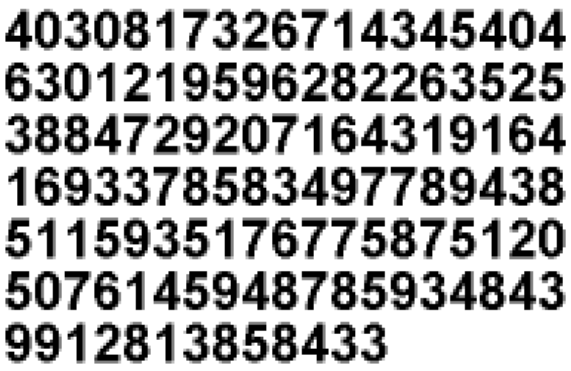
Figure 5. User Interface for Signcryption scheme using Fractal Image Coding software

D. Example

This is an illustration example for the captured image IM Figure 6-A, and the approximate image IM1 using fractal image decoding Figure 6-B.



(A) Image IM created from sent information



(B) Image IM1 created using Fractal image decoding

Figure 6 (A,B). The captured and the generated image

VI. Analysis and Discussion

The two fundamental cryptographic tools (encryption and digital signature) can guarantee the unforgeability, integrity, and confidentiality of communications. They have been considered as distinct building blocks of various cryptographic

systems. Not all messages require both confidentiality and integrity. Some of them need to be signed only, while the others may need to be encrypted only. In the last few years, a new primitive called signcryption is emerged by Zheng [5], to model a process simultaneously achieving privacy and authenticity. The most significant advantage of signcryption over signature then encryption is the reduction of computational cost and communication overhead. That is mean, Cost(signcryption)<Cost(signature)+Cost of (encryption). Many signcryption schemes are proposed throughout the years, they are offering different level of security in spite of different problems and limitation that each one of them having.

For RSA based signature-then-encryption, the public component e is used for encryption or for signature verification. The main computational cost for RSA based signature then encryption is in decryption or signature generation that generally involves modulo exponentiation with a full size exponent d. With the using of CRT, this computational expense can be reduced to a quarter with a full size exponent.

The security of any cryptosystem has to address two aspects: (1) to protect what, and (2) against whom. For the security of the signcryption schemes these two aspects should be addressed also. With the first aspect the content of the signcryption message should be prevented from being disclosed to a third party other than the sender and the receiver, also to prevent the sender from being masquerade by other parties including the receiver. The second aspect is addressed to consider most powerful attacks that can be faced in practice. The signcryption scheme is considered secure if the conditions mentioned in Section 4 is satisfied, exclude the non-repudiation, because it is not necessary in all the application. Although signcryption allows the receiver to be sure that the message has been delivered by the sender, it does not necessarily enables a third-party to verify this because the verification of the authenticity of the message may involve the receiver's secret key, depending on how the signcryption scheme is built [23]. That is mean it is able to provide both the authenticity and privacy of communicated data.

There are two models of security for signcryption: outsider model, and insider model. In case of public key schemes, they satisfy both the outsider and the insider model because the sender and the receiver do not have the same secret key. In the secure insider model, the security of the signcryption scheme is based on the security of the public key encryption scheme, while its integrity is based on the security of the digital signature scheme. In this paper the security of the proposed signcryption scheme depends not only on the security of the RSA system but also on the security of the hash function and the fractal attractor. The authenticated values (hash function values) are one-way values. The one-way property helps to ensure that the message cannot be recovered from the authenticated value easily, so it is considered as a factor to strengthen the security of the protocol.

The security of fractal function is due to their complicated mathematical structure, specifically their recursive construction; they have become a powerful and useful tool in the applied sciences. A part from their advantage, are in storing only few parameters, they provide better approximates than their classical non-recursive counterparts. Based on the fractal properties, which ensure a sufficient level of randomness, high compression capability, and good reduction in the computation cost through using fractal image coding scheme, this method is used for proposing new signcryption scheme. The fractal image that generates through the given parameters needs a great amount of iterations to converge into an attractor, but at the same time, it provides non uniform randomness and it is independent of the image size. This system is robust to attacks for two reasons. Firstly, the attacker manages to obtain parts of the key (or almost the entire key) but a small digit is missing or the order of the affine mappings is changed, the image is changed dramatically. In this case the attacker has no way of extrapolation the rest of the key. Secondly, the brute force attack will not work since a fractal key is time consuming to generate, especially, due to their open key space and big key size.

In addition to the low cost of signcryption schemes regarding to the cost of the signature followed by the cost of encryption, the choice of the key size is also becomes a crucial issue, and plays the main role in the security of digital signature protocol. To ensure the hardness of the problem and to prevent some known attacks the key size must be big. The key space depends on the size of the key. For any chosen number of bits (n), the fractal key space includes 2^n possible key values, while the number of possible keys for RSA is limited to the number of primes in Z_p where p is the largest n-bits prime. The known protocols such as DH and RSA have the advantage of using public–private key, but they are considered as secure systems due to the use of very big prime numbers. For typical security parameters for high level security applications (size of public modulo i = 1536 bits), signcryption costs 58% (50%, respectively) less in computation time and 85% (91%, respectively) less in message expansion than does \signature followed by encryption" based on the discrete logarithm problem (factorization problem, respectively). Therefore, the proposed system provides sufficient level of security, and good reduction in computational cost.

The efficiency of the signcryption scheme is examined in term of the execution time using the same key size. The performance comparison between this scheme and the signature verification scheme is accomplished to conclude that, the former perform better than the later, but the difference is intangible, because the FIC is controlled the overall excursion time, as shown in table 1. Although, this parameter is not considered as a main performance parameter, the security performance is considered as a main parameter in evaluating the proposed method, because it provides a better security performance than the signature verification method.

For image encryption, security depends on two aspects, cryptographic security and perceptual security [24]. The

former one denotes the encryption algorithms security against cryptographic attacks such as brute-force attack, statistical attack, differential attack, etc. The latter one denotes the unintelligibility of the encrypted image content. The security level is high because the jointly coded images cannot be correctly reconstructed without all the required information.

One of the weak points in the proposed system is the use of the OCR code that might give wrong information reading for the generated image, which is not an explicit but approximate image.

Table I

Performance comparisons for the two proposed scheme

No. of Bits	Signature Verification Time in (ms)	Signcryption Time in (ms)
256	4920205	4920003
512	5433936	5433140
1024	7231456	721432
2048	13400231	13400015
4096	24309567	24308423
8192	40657190	40652357

VII. Conclusion

The proposed signcryption scheme in this paper has been based on RSA public key cryptosystems which is considered as a computationally hard problem. This scheme is introduced to satisfy secure and authenticated message delivery that can be fulfilled using the functions of digital signature and encryption separately. The secure transaction for the data between the sender and the receiver could be more protected using fractal compression capability. Fractal image coding and encoding scheme is used to capture the transaction data in a binary image. This image is sent as IFS codes after applying FIC scheme. The received code is used to generate fractal attractor image approximated to the original captured one, using fractal image decoding process. The information is read from the generated attractor using OCR system in order to be verified with the hashed message. The proposed signcryption scheme is simultaneously fulfills both the function of digital signature and public key encryption in a logically single step, and with a cost significantly smaller than that required by signature then encryption.

References

[1] R. Alvarez, F. M. Martinez, J. Vicent, A. Zamora, "A Matricial Public Key Cryptosystem with Digital Signature", *WSEAS Transactions on Mathematics*, vol.7, no.4, pp:195-204, 2008.

[2] W. Diffie and M. Hellman, "New directions in cryptography", *IEEE Trans. Inform. Theory,* vol. 22, no.6, pp. 644–654, 1976.

[3] P. Fei, Q. Shui-Sheng and L. Min. "A Secure Digital Signature Algorithm Based on Elliptic Curve and Chaotic Mappings", *Circuits, Systems, and Signal Processing,* vol. 24, no. 5, pp. 585-597, 2005.

[4] A.M. Jaafar, A. Samsudin, "Visual Digital signature scheme: A New Approach", *IAENG International Journal of computer sciences*, vol. 37, no. 4, 2010.

[5] Y. Zheng. "Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) +cost (encryption)", In: CRYPTO'97, LNCS 1294, pp.165-179. Springer Verlag, 1997.

[6] P. R. Massopust, "Fractal functions and their applications," *Chaos, Solitons and Fractal* ,vol. 8, no.2, pp.171-190, 1997.

[7] N. Al-Saidi, Md. R. M.d Said, "Improved Digital Signature Protocol Using Iterated Function Systems", *International Journal of Computer Mathematics*, vol.88, no.17, pp. 3613-3625,2011.

[8] K. Huang, H. Yan, "Signature Verification using Fractal Transformation", *Proc. of the 15th International Conference on Pattern Recognition*, 2000.

[9] M. F. Barnsley and S. Demko, "Iterated function systems and the global construction of fractals", In proceedings *of the Royal Society of London*, A399, pp. 243-275, 1985.

[10] M. F. Barnsley and L. P. Hud, *Fractal Image Compression*, AK Peters, Ltd., Wellesley, Massachusetts, 1993.

[11] A. Jacquin. "An introduction to fractals and their applications in electrical engineering", *Journal of the Franklin Institute,* vol.331, no.6, pp. 659-680, 1994.

[12] M.F. Barnsley, *Fractals everywhere*. 2nd ed. Academic Press Professional, Inc., San Diego, CA, USA, 1993.

[13] S. Nikiel, *Iterated Function Systems for Real-Time Image Synthesis*, Springer-Verlag London Limited, 2007.

[14] Y. Fisher, *Fractal image compression: theory and application*. Springer-Verlag, New York, 1995.

[15] W. Yung-Gi, H. Ming-Zhi, Yu-Ling Wen, "Fractal Image Compression with Variance and Mean", *ICME,* 2003.

[16] N. Al-Saidi, "Signature verification based on fractal coding scheme", *Proceeding of the 16th WSEAS International Conference on Computer*, Greece 14-17 July, 2012.

[17] W. Stallings' *Cryptography and Network Security: Principles and Practice*, Prentice Hall. 5th Edition, 2010.

[18] M. Tuba, "Digital Signature and Hash Function Irregularity", *Proceeding of the 8th WSEAS international conference on Telecommunications and Informatics*, Turkey May30 –June 1, 2009.

[19] Sk. Md. M. Rahman, S.M. Masum, M.S.I. Khan, M.S. Alam, and M.I. Hasan, "A New Message Digest Function for Message Authentication", *WSEAS Transactions on Computers*, vol. 3, no. 5, pp. 1466-1469, November 2004.

[20] S. Vicky, H. Heather, and S. Samantha, "Optical Character Recognition and the Visually Impaired'. *American Foundation for the Blind*, vol. 59, pp. 1-10, 2006.

[21] M.Toorani, A.A. Beheshti, "Cryptanalysis of an efficient signcryption scheme with forward secrecy based on elliptic curve". *Proceeding of International conference on computer and Electrical Engineering (ICCEE'2008),* pp.428-432, Dec. 2008.

[22] L.Savu, "Digital Signature and Encryption in a Single Logical Step', *In proceeding of the 5th WSEAS International Conference on Communications and Information Technology Stevens Point*, Wisconsin, USA, 2011.

[23] Y. Zheng, Alexander W. Dent, Moti Yung, *Practical Signcryption*, Springer verlag, Berlin, 2010.

[24] N. Al-Saidi, Md. R. M.d Said, and A. M. Ahmed, "Efficiency Analysis for Public Key Systems Based on Fractal Functions". Journal of Computer Science, Vol. 7, No.4, 2011, pp. 526-532.

Nadia M. G. Al-Saidi was born in Iraq 1967. She completed the Bachelor of Science and Master of Science degrees in applied mathematics, from applied sciences department, university of technology, Baghdad, Iraq in 1989, and 1995, respectively. In 2003, she received the Ph.D. degree in fractal geometry from the department of mathematics and computer application sciences in Al-Nahreen university, Baghdad, Iraq. In 1989 she joined the applied sciences department, university of technology, as a staff member, then within 1995-1999 as a lecturer,

whereas she is now Associate Professor since 2003. From 2008-2010, she joined the Institute for Mathematical Research (INSPEM), University Putra Malaysia (UPM) as a post doctorate follow researcher. Her research interests are Cryptographic system based on fractal theory.
Dr. Nadia is the author of numerous technical papers since 1994, she has been a member of the editorial board of some national and international journals, and a member of some professionals societies such as IEEE, Iraqi society of physics and mathematics.