Volume 3, Issue 5, May 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Raising Security of Fingerprint Biometric Systems- using Advanced Encryption Scheme

Dr. Chander Kant
Department of Computer Science and applications, K.U. Kurukshetra, INDIA

Raksha
Department of Computer Science and applications, K.U. Kurukshetra, INDIA

Abstract— Securing biometrics databases from being compromised is major challenge, it must be overcome in order to support widespread use of biometrics based authentication. In this paper we present a cryptographic technique for enhanced security of fingerprint information using RC4 enrichment algorithm approach. RC4 algorithm is already used for image encryption. This paper is about encryption and decryption of images using a stream cipher called RC4, to increase fingerprint security and improved performance. We have also proved the efficiency of proposed approach using simulation in MATLAB.

Keywords— : biometrics, computer security, encryption, decryption, information security, stream ciphers.

I. INTRODUCTION

The advancements in biometric technology have served as a boon in the prevention, detection and solution of crime. Increased security threats in the cities of all countries and the world have highlighted the importance of using biometric technology to prevent crime and bring perpetrators to justice. Biometric technology is becoming most important security technology in today's IT world[4]. In the past few years the security and integrity of data is the main concern. In the present scenario almost all the data is transferred over computer networks due to which it is vulnerable to various kinds of attacks. To make the data secure from various attacks and for the integrity of data we must encrypt the data before it is transmitted or stored. Government, military, financial institution, hospitals and private business deals with confidential images about their patient (in Hospitals) , geographical areas(in research) ,enemy positions (in defense), product , financial status. Most of this information is now collected and stored on electronic computers and transmitted across network to other computer. If these confidential images about enemy positions, patient and geographical areas fall into the wrong hands, then such a breach of security could lead to declaration of war, wrong treatment etc[11]. Protecting confidential images is an ethical and legal requirement. We store information in computer system in the form of files. File is considered as a basic entity for keeping the information. Therefore the problem of securing image data or information on computer system can be defined as the problem of securing file data. It is word wide accepted fact that securing file data is very important, in today's computing environment. Cryptography is a method of storing and transmitting data in a form that only those, it is intended for can read and process. It is a science of protecting information by encoding it into an unreadable format. It is an effective way of protecting sensitive information as it is stored on media or transmitted through network communication paths. To encrypt the data various cryptographic algorithms such DES, 3DES, blowfish, AES, RC4 etc are used [2]. So we are implementing RC4 algorithm fastest in data processing/storing compare to other algorithms which is mentioned above. RC4 is highly secured because it can operate up to a key length of 2048 bits[5]. The main aim behind the design of this proposal is to get the best security/performance tradeoff over existing ciphers.

This paper is organized as follows:

- In Section 2, we describe the background of fingerprint biometric systems, their effectiveness requirements followed by encryption basics.
- Section 3 presents a classification of stream cipher based encryption techniques.
- Section 4 proposes a scheme with the help of stream based encryption method i.e. using Rc4 to enhance the security of fingerprint biometric systems.
- Section 5 gives the concluding remarks along with the future aspects.

II. FINGERPRINT SYSTEMS BACKGROUND

A. Fingerprint as Biometrics traits

Fingerprint-based identification is one of the oldest method among all the biometric techniques, which has proved its use successfully in numerous applications. Everyone is known to possess a unique, immutable characteristic i.e. fingerprints. The uniqueness of a fingerprint is determined by the pattern of ridges and furrows as well as the minutiae points. A smoothly flowing pattern formed by ridges and furrows on the hand is called a palm print. A fingerprint is believed to be unique to each person. Fingerprints of even identical personalities namely twins are different. Fingerprints are one of the

most oldest biometric technologies and are considered as proofs of evidence in courts of law all over the world. That's why these are used in forensic divisions worldwide for criminal investigations.

The analysis of fingerprints for matching purposes generally requires the comparison of several features of the print pattern. These include patterns, which are aggregate characteristics of ridges, and minutia points, which are unique features found within the patterns. It is also necessary to know the structure and characteristic features of human skin in order to successfully employ some of the imaging technologies[1].

Fingerprint Patterns

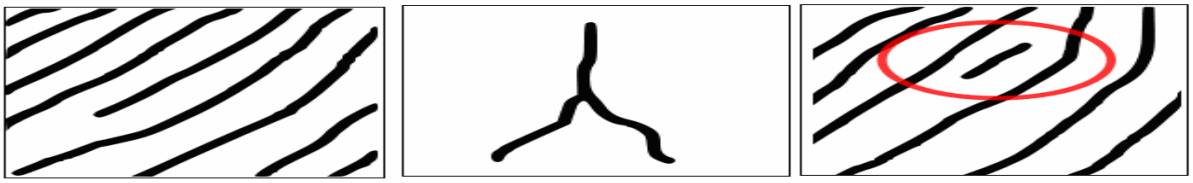
The three basic patterns of fingerprint ridges are the arch, loop, and whorl as shown in Figure 1.1. An arch is a pattern where the ridges enter from one side of the finger, rise in the center forming an arc, and then exit the other side of the finger (Fig 1.1 a). The loop is a pattern where the ridges enter from one side of a finger, form a curve, and tend to exit from the same side they enter (Fig 1.1 b).

(a) Arch (b) Loop (c) Whorl

In the whorl pattern, ridges form circularly around a central point on the finger (Fig 1.1 c). Scientists have found that family members often share the same general fingerprint patterns, with the belief that these patterns are inherited[3].

Minutia Points

The major Minutia points in fingerprint are: ridge ending, bifurcation, and short ridge or dot as shown in Figure 1.2.



(a) Ridges Ending (b) Ridges Bifurcation (c) Dot

Figure 1.2 Minutiae points in fingerprint

The ridge ending is the point at which a ridge terminates (Fig 1.2 a). Bifurcations are points at which a single ridge splits into two ridges (Fig 1.2b). Short ridges or dots are ridges which are significantly shorter than the average ridge length on the fingerprint[3] (Fig 1.2 c). Minutiae and patterns are very important in the analysis of fingerprints since no two fingers have been shown to be identical.

Fingerprint Matching

A fingerprint is made up of a series of ridges and furrows on the surface of the finger. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points[6][8]. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending. Fingerprint matching techniques can be divided into two categories: minutiae-based and correlation based. Minutiae-based techniques first find minutiae points and then map their relative placement on the finger[10] as shown in Figure 1.3

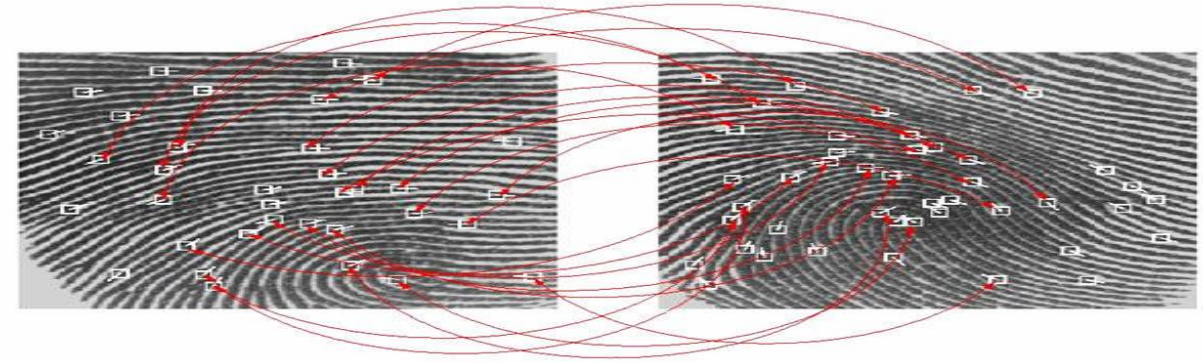


Figure 1.3 Matching minutiae points in two fingerprints

However, there are some difficulties when using this approach. It is difficult to extract the minutiae points accurately when the fingerprint is of low quality. Also this method does not take into account the global pattern of ridges and

furrows. The correlation-based method is able to overcome some of the difficulties of the minutiae-based approach. However, it has some of its own shortcomings. Correlation-based techniques require the precise location of a registration point and are affected by image translation and rotation. Fingerprint matching based on minutiae has problems in matching different sized (unregistered) minutiae patterns. Local ridge structures cannot be completely characterized by minutiae. A commercial fingerprint-based authentication system requires a very low False Reject Rate (FAR) for a given False Accept Rate (FAR).

B. Encryption Basics

Cryptography is the science of encrypting a plaintext such that it is rendered unreadable to others except the person for whom the message is intended. It involves two processes of encryption and decryption [8].In cryptography, encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it, but that authorized parties can. In an encryption scheme, the message or information (known as plaintext) is encrypted using an encryption algorithm, which gives rise to unreadable cipher text. This is done with the help of an encryption key, specifying how the message is to be encoded. Having a look at the cipher text any adversary should not be able to determine anything about the original message. An authorized party, however, is able to decode the cipher text using a decryption algorithm, which requires a secret decryption key, that adversaries do not have access to[7].

III. STREAM CIPHERS CLASSIFICATION

In cryptography, a stream cipher is a symmetric key cipher where plaintext digits are combined with a pseudorandom digit stream (i.e. key stream). In a stream cipher each plaintext digit is encrypted one at a time with the corresponding digit of the key stream, to give a digit of the cipher text stream. In practice, a digit is typically a bit and the combining operation an exclusive-or (xor).

A stream cipher generates successive elements of the key stream based on an internal state. This state can be updated in two ways as[12]:

- if the state changes independently of the plaintext or cipher text messages, the cipher is classified as a synchronous stream cipher.
- In contrast, if stream ciphers update their state based on previous cipher text digits, it is called self-synchronizing cipher.

1) A. Synchronous stream ciphers[12]

In a synchronous stream cipher a stream of pseudo-random digits is generated independently of the plaintext and cipher text messages, and then combined with the plaintext (to encrypt) or the cipher text (to decrypt). Generally, binary digits(bits) are used , and the key stream is combined with the plaintext using the exclusive or operation (XOR). This is termed a binary additive stream cipher.

In a synchronous stream cipher, the sender and receiver must be exactly in step for decryption to be successful. If digits are added or removed from the message during transmission, there is a loss of synchronization. In order to restore the lost synchronization, various offsets can be tried systematically to obtain the correct decryption. Another approach can be to tag the cipher text with markers at regular points in the output.

If, however, a digit is corrupted in transmission, rather than added or lost, only a single digit in the plaintext is affected and the error does not propagate to other parts of the message. This property is useful when the transmission error rate is high; however, it makes it less likely the error would be detected without further mechanisms. Moreover, because of this property, synchronous stream ciphers are very susceptible to active attacks: if an attacker can change a digit in the cipher text, he might be able to make predictable changes to the corresponding plaintext bit; for example, flipping a bit in the cipher text causes the same bit to be flipped in the plaintext.

2) B. Self-synchronizing stream ciphers[12]

Another approach uses several of the previous *N* cipher text digits to compute the key stream. Such schemes are known as self-synchronizing stream ciphers, asynchronous stream ciphers or cipher text auto key (CTAK). The idea of self-synchronization was patented in 1946, and has the advantage that the receiver will automatically synchronize with the key stream generator after receiving *N* cipher text digits, making it easier to recover if digits are dropped or added to the message stream. Single-digit errors are limited in their effect, affecting only up to *N* plaintext digits[9,12].

An example of a self-synchronizing stream cipher is a block cipher in cipher feedback(CFB) mode.

TABLE 1

COMPARISON TABLE OF VARIUS STREAM CIPHERSTHAT CAN BE APPLIED OVER FINGERPRINT BIOMETRIC SYSTEMS[14].

Stream Cipher	Creation Date	Speed (cycles per byte)	(bits)			Attack	
			Effective Key-Length	Initialization vector	Internal State	Best Known	Computational Complexity
A5/2	1989	Voice (W phone)	54	114	64?	Active	4.6 milliseconds

FISH	1993	Quite Fast (W_{soft})	Variable	**?**	**?**	Known-plaintext attack	2^{11}
Rabbit	2003-Feb	3.7(W_{P3})-9.7(W_{ARM7})	128	64	512	N/A (2006)	
RC4	1987	7 W_{P5}[1]	8-2048 usually 40-256	8	2064	Shamir Initial-Bytes Key-Derivation OR KPA	
Scream	2002	4 - 5 (W_{soft})	128 + a 128-bit Nonce	32?	64-bit round function	**?**	
SEAL	1997	Very Fast (W_{32-bit})	**?**	32?	**?**	**?**	

C. RC4 Basics:

The most proposed approach for the image encryption is RC4 stream cipher. The reason, RC4 stream cipher is speedy encrypt image, less resources used, less time and implementation complexity.RC4 stream cipher is the most preferred Stream cipher algorithm[7][9]. In the RC4 algorithm, there are two stages process during encryption as well as decryption. The algorithm is divided into the two parts KSA (Key scheduling Algorithm) and PRGA (Pseudo Random Generator algorithm). KSA as the first stage of algorithm also knows as initialization of S (s is state vector) and PRGA known as stream generation in the RC4 whole process[7][9].

In the first stages of RC4 Stream Cipher algorithm on the bases of variable sized key from 1 to 256 a State Vector (State Table) of fixed length 256 bytes is generated, after on the base of State Table, we generate the key stream that XOR with plaintext and cipher text during encryption and decryption. During encryption the key stream is XOR with the plaintext and during decryption the cipher text XOR with key stream then convert into the plaintext. In the description of RC4, first we discussing the first stage of the algorithm known as KSA, in this stage following steps are done:

1. Inputting the variable length key of size from 1 to 256
2. Initialize the key matrix as per the size of the input key
3. Initialize the State table of fixed size 256 bytes from the value 0 to 255 in ascending order.
4. Using the key matrix of variable size done the permutation on the S table
5. Output of the KDA, the final prepare S table after shuffling operation.

In this manner the KDA generate the State Table (State Matrix) of 256 bytes.

Now, let's discuss the algorithm of the KDA as following

KSA

1. for i=0 to N-1
2. s[i]=1
3. j=0
4. for i=0 to N-1
5. j=(j+s[i]+k[i]) mod N
6. swap(s[i],s[j])

Thereafter, we discuss the second stages of the algorithm known as PRGA These stages basically used to generate the output key stream that used to encrypt and decrypt the data by XORed operation.

The algorithm description the algorithm as following

PRGA

1. i=j=0
2. Loop
3. i=(i+1) mod N
4. j=(j + s[i]) mod N

5. swap(s[i],s[j])
6. output= s[s[i] + s[j]] mod N] .

IV. **PROPOSED SCHEME**

After considering a number of encryption algorithms categorized under stream cipher's, this encryption scheme i.e. RC4 encryption can be generalized over fingerprint biometric systems.

This scheme is expected to give good results in fingerprint biometrics particularly, as their application has already been tested over various random image samples. Moreover, in case of forgery of biometric templates like fingerprint images by unauthorized people this scheme is going to be very effective approach. A number of characteristics which contribute to the successful application of the purposed schemes comes with the advantages of stream ciphers as[11]:

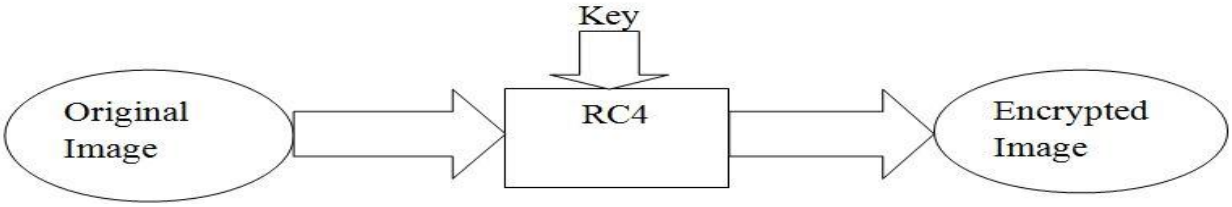
- The key stream is generated independently of the message stream.
- Less vulnerable to insertion and deletion of blocks.
- Easy to analyze mathematically.
- Less susceptible to crypto-analysis.

Having a number of positive qualities, we can blindly think to apply the well known stream cipher algorithm named as RC4 over fingerprint sample images to prevent their acquirement and forgery by unauthorized people. An image once encrypted using RC4 can be stored into the database safely, and becomes difficult to recover by an intruder. Moreover, by applying some changes over the data to be stored into the database in spite of entering it as it is, makes our database less vulnerable to the attacks.

A. *Image encryption and Decryption Processes Using RC4*

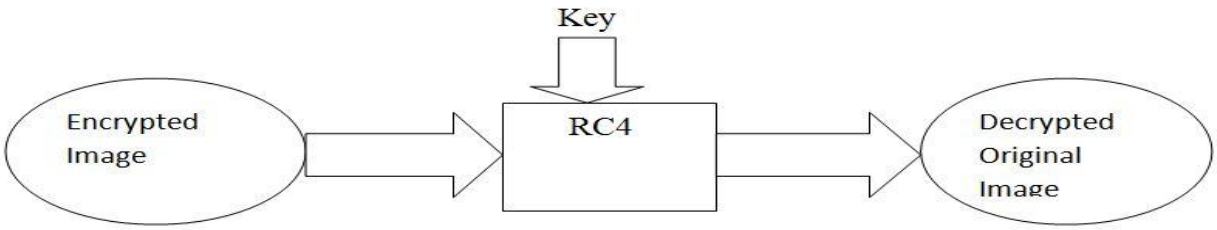
Encryption Process

Data image as a plaintext and the encryption key are two inputs of encryption process.

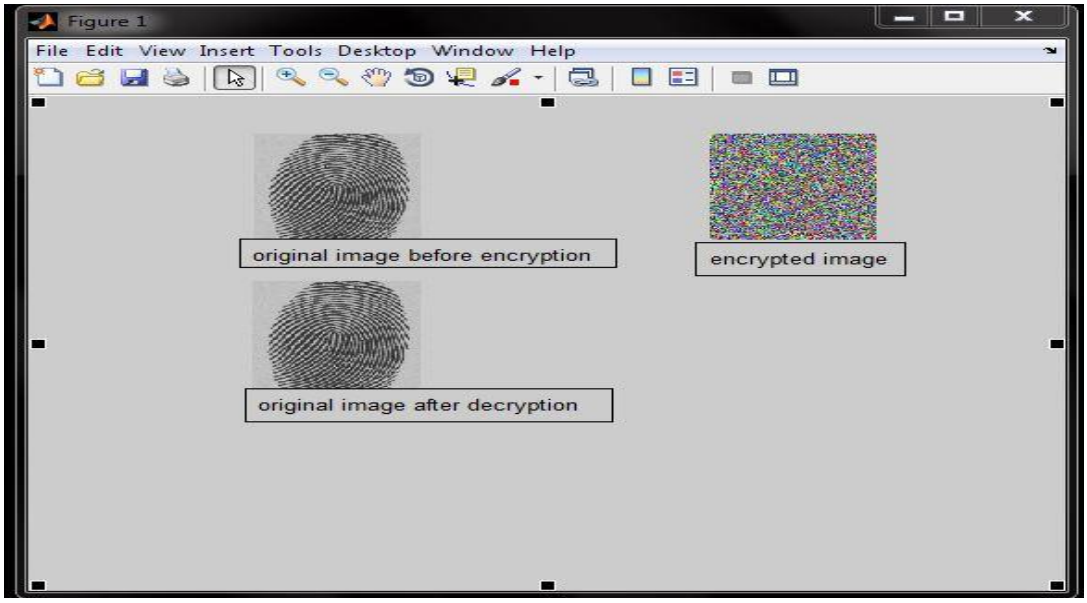


Decryption Process

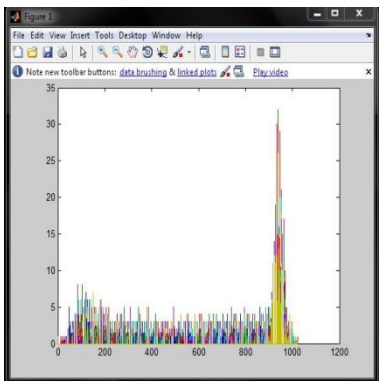
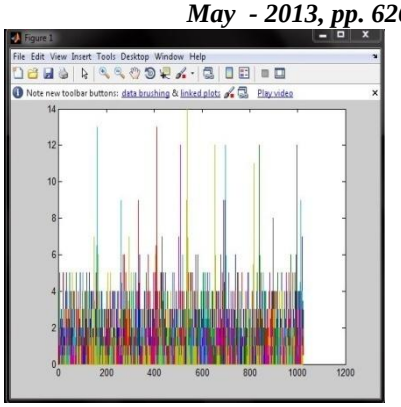
Decryption process uses the same key and algorithm to generate the original image.



B. *Matlab Oriented Results:*



The above result shows the original image, encrypted image and the decrypted image. We can clearly see that the decrypted image is same as the original image after applying RC4 in reverse direction from encrypted image.

1.Original and encrypted image | 2. Histogram of original image | 3. Histogram of Encrypted image

Different fingerprint samples have been tested by the proposed encryption idea. It is clear that the histogram of the encrypted image is more dynamic and significantly different from the histogram of original image. So, encrypted image does not provide any clue to employ any statistical attack on the proposed encryption of an image. These properties tell that proposed image encryption has high security against statistical attacks.

V. CONCLUSION AND FUTURE WORK

Cryptography is widely used due to the upcoming trends of security in internet and wireless[13][15]. Further work is possible in this area by combining more such ciphers. Ciphers can be combined to make them more secure, more usable and effective. This technique can be further used in all spheres wherever encryption is needed. This paper discusses how to encrypt fingerprint image securely within a short time using the stream cipher. This can be further extended to other forms of data such as audio video transmissions which also require high security but without the overhead of extra time taken for encryption. In future fingerprint security can be raised by the joint application of more than one stream based cipher

References

[1] A. Abhyankar and S. Schuckers, "Towards integrating level-3 features with perspiration pattern for robust fingerprint recognition", in *17th International Conference on Image Processing*, Hong Kong, 2010.

[2] A. Nagar, K. Nandakumar, and A. Jain, "A hybrid biometric cryptosystem for securing fingerprint minutiae templates," Pattern Recogn. Lett., vol. 31, pp. 733–741, 2010.

[3] B. Tan and S. Schuckers, "Spoofing protection for fingerprint scanner by fusing ridge signal and valley noise", *Pattern Recognition*, 2010.

[4] F. Chafia, C. Salim, and B. Farid, "A biometric crypto-system for authentication," in Proc. of Int. Conf. on Machine and Web Intelligence (ICMWI), 2010, pp. 434–438.

[5] *Hameed A. Younis*, Dr. Turki Y. Abdalla**, Dr. Abdulkareem Y. Abdalla*, "*A Modified Technique For Image Encryption*".*

[6] H. Xu and R. N. Veldhuis, "Binary representations of fingerprint spectral minutiae features," in Proc. of the 20th Int. Conf. on Pattern Recognition (ICPR'10), 2010, pp. 1212–1216.

[7] Jian Xie, Xiaozhong Pan, "An Improved RC4 Stream Cipher ", International Conference on Computer Application and System Modeling (ICCASM), 2010.

[8] K. Nandakumar, "A fingerprint cryptosystem based on minutiae phase spectrum," in Proc. of IEEE Workshop on Information Forensics and Security (WIFS), 2010.

[9] Lepakshi goud.T, Dynamic routing with Security using a Blow fish Algorithm in the multiple Organizing system, IJAEST, vol No .4,issue No 1, 2011,1-9.

[10] M. Barni, T. Bianchi, D. Catalano, R. M. Di, L. R. Donida, P. Failla, D. Fiore, R. Lazzeretti, V. Piuri, F. Scotti, and A. Piva, "Privacypreserving fingercode authentication," in Proc. of the 12th ACM workshop on Multimedia and security, ser. MM&Sec '10, 2010, pp. 231–240.

[11] M. Espinoza, C. Champod and P. Margot, "Vulnerabilities of fingerprint reader to fake fingerprints attacks", *Forensic Science International*, vol. 204, pp.41-49, 2011.

[12] Pardeep,Pushpendra, **"**A Pragmatic Study on Different Stream Ciphers And On Different Flavors of RC4 Stream Cipher**",** 2012.

[13] "SPEED (Signal Processing in the EncryptEd Domain) project," URL: http://www.speedproject.eu/, retrieved April, 2011.

[14] Simar Preet Singh, Comparison of Data Encryption Algorithm, IJCSC, Vol 2 No.1, June-2011,pp 125-127

[15]. Sapna Sasidharan and Deepu Sleeba Philip, "A FAST PARTIAL IMAGE ENCRYPTION SCHEME WITHWAVELET TRANSFORM AND RC4", 2011

