A New Cryptosystem based on Fingerprint Features

Tarik Zeyad Ismaeel, PhD
University of Baghdad
Electrical engineering department
Baghdad, Iraq

Ahmed Saad Names
University of Baghdad
Electrical engineering department
Baghdad, Iraq

ABSTRACT
Data encryption has become more important in the world of information, in order to secure the information during communicating or transmitting and to prevent an illegal person from achieving on the sensitive information. In this paper, fingerprint encryption algorithm is proposed which is used to encrypt data. Fingerprint image is used to generate three types of fingerprint keys which are derived from different types of fingerprint features. These keys are (bifurcation, ending and minutiae keys).

The proposed fingerprint encryption algorithms use the fingerprint keys and table in encryption and decryption process. This method used the fingerprint key with a simple equation in order to generate the encryption key. The encryption key used to encrypt and decrypt data.

The results show three different cipher texts in hexadecimal form which are encrypted by using the new algorithm. The differences among these texts are very large. The large differences due to use a larger look up table with (256×256) dimensions in encryption. The simulation results of the new encryption method give high security with a good performance.

Keywords
Encryption, decryption, plaintext, ciphertext, fingerprint.

1. INTRODUCTION
Data security became more important to personal computer for protection of information. Therefore, security problems become important issues for the internet. So that the encryption algorithms, which are also called cryptography algorithms, are used to protect data and improve security. Encryption is the capability to securely saving and transmitting important data. Encryption, to most human, is interested with guarding the privacy of communications. Encryption means hiding a message in transmitter by converting it into an incomprehensible form by using ciphering and then recovering to understandable form by using deciphering [1].

The goal of protecting text by converting the encrypted messages into an unreadable format, called cipher text. Only person who has an encryption key can decrypt or decipher the cipher text in to original text [2]. Sometimes, encrypted message can be broken by "cryptanalysis" which it's called keys of breaking. In general, data is first encrypted into another form and then transmitted. Thus, in any encryption system there are three steps which are as follows:

At first a data is encrypted, then data is transmitted which contains a secret key, at last the cipher text is decrypted using secret key [3].

When the encryption key is the same as the decryption key, the process is called as symmetric encryption; otherwise, it is called asymmetric encryption. [4].

All types of encryption algorithms have five parameters which are plain text, ciphering

(Encryption) algorithms, encryption key, ciphertext, and deciphering (decryption) algorithms.

In any encryption algorithm there are many conditions that should be followed, which are as follows:

The strong encryption algorithm is needed, i.e. at a minimum, if an illegal person who gets the encryption algorithm and many cipher texts will be unable to decrypt the cipher text or conclude the encryption key. The second requirement, the encryption key must be unbreakable. The recipient and sender must keep the encryption key secure. If someone can conclude the encryption key and knows the encryption algorithm, all information which are encrypted by using this algorithm will be readable.

The strength of an encryption algorithm depends on the strength of the public and secret keys [5]. In the general encryption algorithms, such as AES "advanced encryption standard", DES "data encryption standard" and RSA "Rivest_Shamir_Adleman" etc., data is ciphered by use secret key.

Also the biometric key is used in encryption algorithms to get on the stronger key. The biometrics can be defined as a measurable, unique, biologically characteristics or traits that using for automatic ""verifying and recognizing the person identity. This biologically characteristic has been called as the biometrics science [6]. Biometrics are unique for every person. Mostly biometrics features which are used for security purpose such as fingerprints, palms, face, iris's, retina, etc.

The fingerprint is a one off the most common physically biometrics patterns analyzed which is used for encryption purposes. Usually, fingerprint algorithms are used to analyze the person characteristic for security or encryption purposes [7].

The new proposed encryption algorithms uses fingerprint key in the encryption process, which is uses the fingerprint features in generating the encryption key, this type of key can increase the robustness of this algorithm [8].

The fingerprint encryption gives a develop method for key encryption by employing a fingerprint in order to generate the encryption keys, Instead of using a passwords to get the encryption keys. If an individual wants to get an encryption key he will put a fingerprint on the scanner to allow for the capture of a fingerprint sample in order to generate the fingerprint key. Then the key is used to cipher or decipher information. The passcodes keys are replaced by the

fingerprint key to protect information in order to offer both secure ID accentuation and accession [5].

2. FINGERPRINT

A fingerprint is a pattern which contains a feature in the finger as shown in the figure (1) [9]. In general, it is believed that each fingerprint in this world is unique and so each person in this world has a unique fingerprint with a permanent unique characteristics over it [10]. Therefore, the fingerprints are used for various forensic investigation, security and identification from a long period of time.

The fingerprint is not recognized by its ridges and valley, but it is recognized by minutiae, which are stable points that located on the ridges as shown in figure (1). In general, the fingerprints can be classified into many types depending on the global configuration of fingerprint ridge structure, while the features distribution are used in the fingerprint matching by checking a similarity between large of fingerprints. This a unique features are used to implement a fingerprint encryption or authentication systems. These features can be used in recognition of the fingerprint from large quantities of fingerprints by compression among original features and the features of other fingerprints. This system will decide acceptance or rejection of the input fingerprint depending on the matching among the fingerprints and original fingerprint.

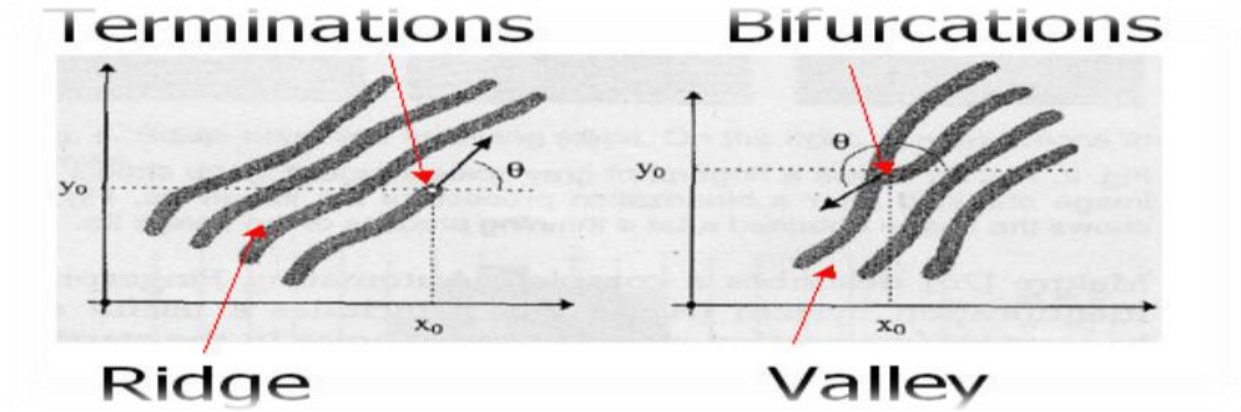

Figure (1) Minutiae (ridge termination and bifurcation).

3. FINGERPRINT IMAGE PROCESSING AND FEATURE EXTRACTION

In order to extract the minutiae from fingerprint, there are three stages that are widely employed by researchers will be used. These stages are pre-processing, minutia-extraction and post-processing stage as illustrated in figure (2) [10]**:**

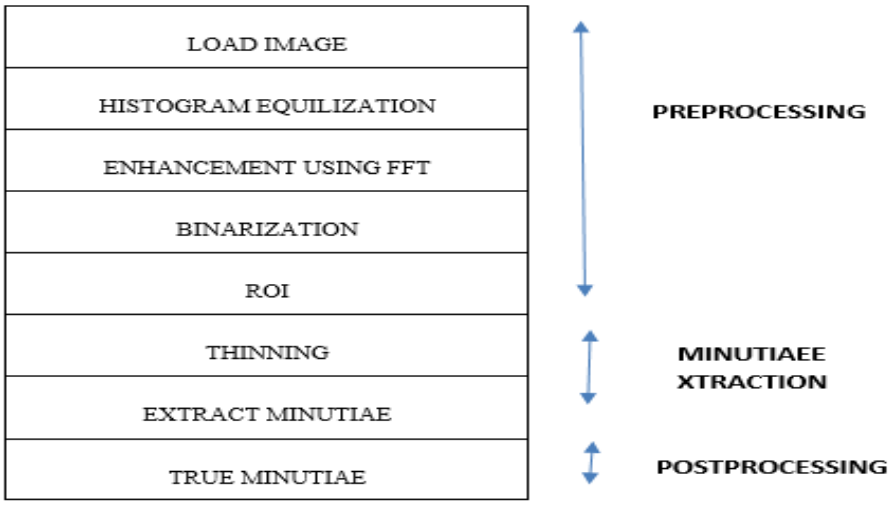

Figure 2.Illustrates the three-stage of a minutia extractor

4. GENERAL ENCRYPTION MODELS

In general, the proposed encryption algorithm will use fingerprint features to generate encryption keys that will be used in these algorithms. The first step will be generating the fingerprint key. Fingerprint key is extracted from fingerprint features which Consists of the most stable elements (ridge ending and ridge bifurcation). Finally, the last step will be proposing the general producers for fingerprint encryption algorithms.

A. Fingerprint key generation

In any encryption algorithm, there are many factors used to check the performance of encryption algorithm. These factors are strength of encryption and speed of encryption algorithm. The strength factor depends on the key strength.

In general, the key strength depends on two parameters. These parameters are the length and the random distribution of key. In order to get a good random distribution of encryption key, the encryption key will be derived from fingerprint features because the features of fingerprint, which are used to generate encryption key, are randomly distributed. The steps of the key generation are as follows:

I. Choosing the type of minutiae that uses for the fingerprint key generation such as minutiae ending, minutiae bifurcation or merging between the two types of key (minutiae key). Figures (3.1.a-3.1.c) illustrate the three types of fingerprint keys.

II. Finding the average point (center point) of this type of minutiae by using the following equations.

$$\bar{X}=\frac{\sum_1^i X_i}{i} \quad \text{.... (1)}$$

$$\bar{Y}=\frac{\sum_1^i Y_i}{i} \quad \text{.... (2)}$$

Where i is the total number of minutiae in fingerprint image and $\bar{X}$, $\bar{Y}$ are the center point (CP) of this minutiae.

III. Finding the length of the distance (Lei) between minutiae and the center point for each minutiae point by using the following equation.

$$Le_i=\sqrt{(X_i-\bar{X})^2+(Y_i-\bar{Y})^2} \quad \text{.... (3)}$$

IV. Normalizing these lengths (Lei) by using the tow following steps.

a. Find the maximum value of length (max Lei).
b. Divide each length on (max Lei) as shown following equation.

$$Lein=Lei/max\ (Lei) \quad \text{.... (4)}$$

Where Lein is the normalized value of Lei.

V. Finding the angle (θi) between each minutiae point and center point by using the following equation.

$$\theta_i=\tan^{-1}\frac{Y_i-\bar{Y}}{X_i-\bar{X}} \quad \text{.... (5)}$$

The resultant angle from above equation is limited between (90º, -90º). The value of θi will be converted to another range (0, 360º) by applying the following steps.

If (Yi-$\bar{Y}$) value is negative and (Xi-$\bar{X}$) is positive. The new value of θi will equals to (360º -old θi).

If (Xi-$\bar{X}$) value is negative. The new value of θi equals to (180º +old θi).

If (Yi-$\bar{Y}$) and (Xi-$\bar{X}$) values are positive. The new value of θi equals to the old value of θi.

Writing the fingerprint key in form of two vectors. These vectors consist of Lein and angle θi.

B. Procedures of encryption and decryption

In general, this stage is more important in an encryption algorithm. This stage consists of two parts. These parts are the encryption and decryption procedures.

I. Encryption procedures

In general, the efficiency of an encryption algorithm depends on encryption procedures. There are two factors used to measure the performance of encryption procedures which are the speed of encryption and decryption algorithm and the probability of breaking the algorithm. The procedures of the encryption algorithm are as follows:

a. Converting the data that will be encrypted to binary form.

b. Separating the binary data in to some of gropes each one group consists of 8 bits.

c. Creating empty table which consists of 256 rows and 256 columns. The rows are limited by range of angle ($\frac{(k-1)*360}{256}$ < row (k) ≤ $\frac{(k)*360}{256}$) and the columns are limited by range of length ($\frac{(j-1)}{256}$ < column (j) ≤ $\frac{(j)}{256}$). Where i and j are positive integer number ranges from 1 to 256.

d. Depending on fingerprint key vector (θ_i and Le_in), the rows and columns sequences numbers will be selected, which are used to find a location of encryption key, in the temporary table.

e. Using equation (3.6) to fill the temporary table by the encryption keys ENCK= ((k-1)*265*3+j*3+k*2) mod256 .... (6) Where i and j are the columns and rows numbers of this location.

f. Converting ENCK from decimal form to binary form (ENBK). Each binary number consists of 8 bits.

g. Ciphering data (CD) by using the XOR operation between binary data groups (DG) and encryption keys (ENBK), i.e. CD= XOR (DG, ENBK).

Whole steps of encryption procedures are illustrated in figure (3).

II. Decryption procedures

In general, the decryption procedures of this algorithm are the same as encryption procedures but with replacing the plaintext by the cipher text.

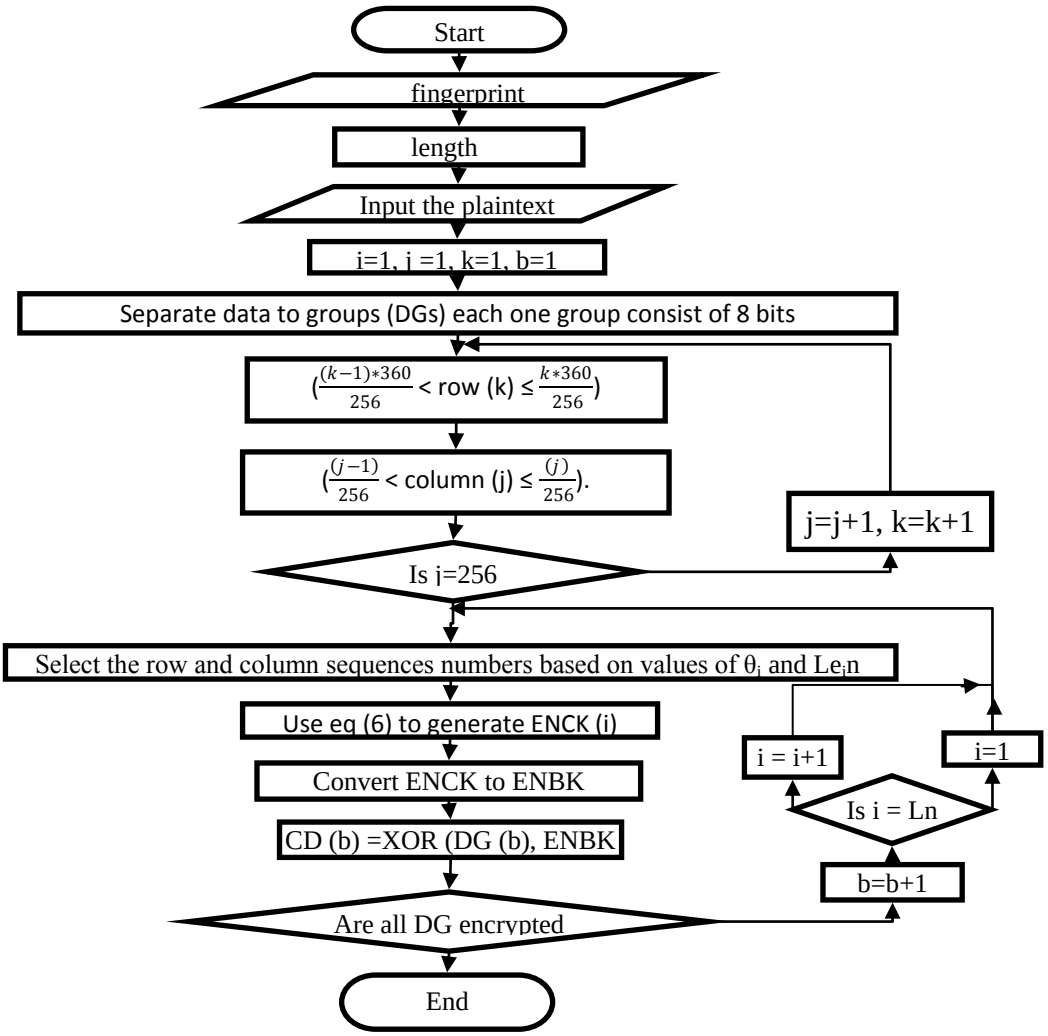

Figure (3): encryption algorithm flowchart

C. Strength of fingerprint key

The strength of this key depends on three parameters. These parameters are the length of the key and numbers of rows and columns in table. Equation (7) is derived to calculate the time of breaking by using a brute force attack.

$$BFT = (Nc^{Lk} * Nr^{Lk})/2000000 \quad .... (7)$$

Where lk is length of fingerprint key. Nc and Nr are number of column and row respectively.

5. EXPERIMENTAL RESULTS AND ANALYSIS

The MATLAB environment is used to implement the new system and also used to analysis the performances of this system.

A. Results of encryption algorithms

The fingerprint keys, which are derived from three minutiae used to encrypt the plain text. two plain text are used to check the performances of system which are shown in example (1).

At first, the fingerprint key, which is derived from bifurcation minutiae is used to encrypt the plaintexts. The results of cipher texts are shown in example (2). These texts in hexadecimal form.

Example (2): cipher texts by using the bifurcation key.

B6C377C2F3E66AF06209D8
E6C377A2A38822065AC9D0BD6663B4704656CB41FAA3408
470DA71FEAB6663E47036B6E36F349B102A063A9978F3

At second, the fingerprint key, which derived from ending minutiae is used to encrypt the plaintexts. The results of cipher texts are shown in example (3).

Example (3): cipher texts by using the ending key.

12A232F2F204EAF24A3222
42A23292A26AA20472F22A04823232049AF2AA04CAA2A20
472F24A041282326204EA12822A049AF2AA0412A2824A

At last, the fingerprint key, which is derived from minutiae key is used to encrypt the plaintexts. The results of cipher text are shown in example (4).

Example (4): cipher texts by using the two minutiae in key generation.

1	E277D80D8BCFF88B2F83D4
2	B277D86DDBA1B07D1743DCDF8F4A9A414B8E5B5 D04E95DA75152ED7C9D5450B54E82588CD63EC58 C57F7B3033A16

The results show the differences among the cipher texts although using the same fingerprint image to generate the fingerprint key at encryption. These differences are caused by using the three types of keys.

B. Results of security strength

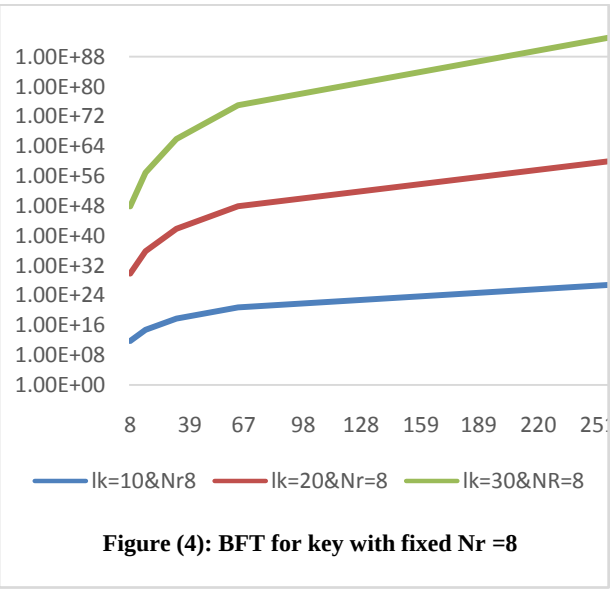

Figure (4): BFT for key with fixed Nr =8

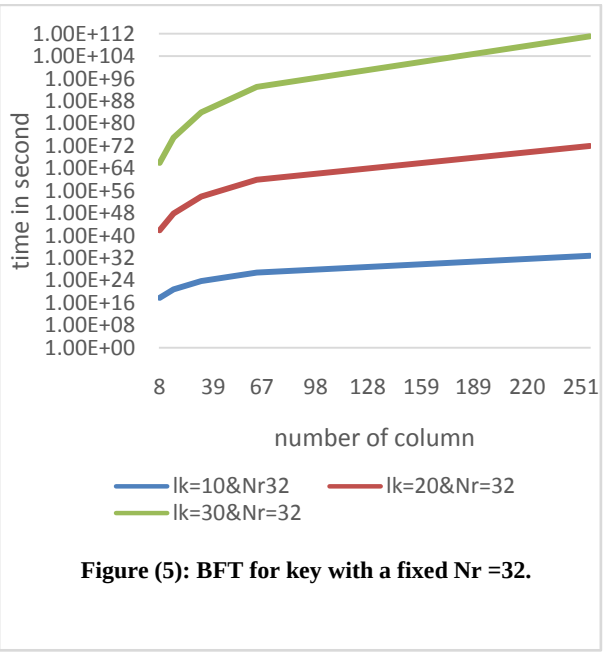

Figure (5): BFT for key with a fixed Nr =32.

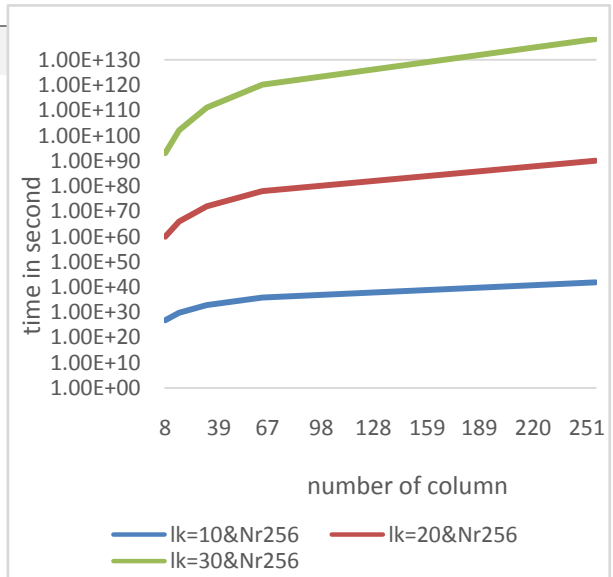

Figure (6): BFT for with a fixed Nr =256.

The strength of security of this algorithm depends on key strength. The key strength depends on three factors which are the number of rows and columns and the length of key as illustrated in equation (7). The simulation results are shown in figures (4-5-6). These figures show the security of key can be increased by increasing the key length or increasing number of rows or columns in table.

6. CONCLUSIONS

This paper proposed a novel fingerprint cryptosystem. The system extracted vector feature from fingerprint and used the modified algorithm to encrypt and decrypt messages

From previous experiments and simulation results, the following issues can be concluded:

1. The new encryption algorithm is effective and have high security for encrypting data. The advantages of these algorithms are: Simple implementation, high security, strong encryption key and the security strength can be increased by changing any one of key parameters.
2. This study has found that the fingerprint key length is more effective on the security than other parameters such columns and rows numbers.

7. REFERENCES

[1] W. Stallings, “Cryptography and Network Security: Principles and Practice 5th Edition”, Prentice Hall, 2010.

[2] K. H. Rosen, “An Introduction to Cryptography 2th Edition”, Taylor & Francis Group, LLC, 2007.

[3] P. P. Palsaniya and P. D. Soni, “Crypto Steganography Security Enhancement by using Efficient Data Hiding Techniques”, International Journal of Application or Innovation in Engineering & Management (IJAIEM), Vol. 3, , Issue. 2, pp. 263-267, 2014.

[4] H. R. Nemati, "Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering", 2010.

[5] C. Soutar, A. Stoianov, Rene Gilroy, and B.V.K Vijaya Kumar, "Biometric EncryptionTM", Proc. SPIE 3314, pp. 178-188, 1998 .

[6] A. Cavoukian, A. Stoianov and F. Carter, "Biometric Encryption: Technology for Strong Authentication, Security and Privacy" International Federation for Information Processing, Vol. 261, pp. 57–77., 2008.

[7] E. J. Kindt, "Privacy and Data Protection Issues of Biometric Applications", Springer, 2013.

[8] K. Martin, H. Lu, M. Bui, N. Konstantinos, D. Hatzinakos, "A Biometric Encryption System for the Self-Exclusion Scenario of Face Recognition", IEEE SYSTEMS JOURNAL, VOL. 3, NO. 4, pp. 440-450, DECEMBER 2009.

[9] V. Awasthi, V. Awasthi, K. K. Tiwari. "Finger Print Analysis Using Termination and Bifurcation Minutiae", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 2, February 2012.

[10] M. Kaur, M. Singh, A. Girdhar, and P. S. Sandhu. "Fingerprint Verification System using Minutiae Extraction Technique", World Academy of Science, Engineering and Technology 46 2008.