Int Jr. of Mathematics Sciences & Applications
Vol.3, No.1, January-June 2013

ISSN No: 2230-9888
www.journalshub.com

Mathematical Model Based Total Security System with Qualitative and Quantitative Data of Human

Sneha K. Patel[1] and Dr. D. C. Joshi[2]
[1] Humanities and Social Science department,
Shree Swami Atmanand Saraswati Institute of Technology, Surat
E-mail: sneha_patel_04@yahoo.co.in
[2]Department of Mathematics
Veer Narmad South Gujarat University, Surat.
E-mail: dilip_joshi2002@yahoo.co.in

Abstract

The present era of information and technology is quickly revolutionizing the way of transactions. Human involvement in handling and authenticating day to day activities is being increasingly replaced by electronic gadgets/systems. This growth in electronic transactions results in a raise of demand for fast and accurate user identification and authentication system. Access codes for buildings, banks accounts and computer systems often use PIN's for identification and security clearances. When credit and ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes. Total security system may solve this problem since a face, speech, fingerprint, palm print etc. are undeniably connected to its owner. This system can compare scans to the records stored in a central or local database or even on a smart card. *The main aim of this paper is to construct mathematical model based on cryptography for total security system using qualitative and quantitative data of human.*
Key words: *Security, Cryptography, Qualitative, Quantitative,* ***Biometrics***

Introduction

The present era of information and technology is quickly revolutionizing the way of transactions. And security is a major part of technology. Access codes for banks accounts and computer systems often use PIN's for identification and security clearances. When credit and ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes. Total security system may solve this problem since a face, speech, fingerprint, palm print etc. are undeniably connected to its owner. We are solving this problem with the help of PCA and RSA Algorithm.

The term data refers to set of variables like the results of measurements, graphs, images etc...There are two types of data qualitative and quantitative. If data is in numerical form then it is known as quantitative data. Otherwise it is known as qualitative data [7]. The quantitative types of data are 'hard', ‘exact’, 'credible', and 'scientific'. Smart card, PIN numbers, login ID and password, keys, passports, all e-cards and so on, can be considered as quantitative data. And the qualitative types of data are 'sensitive', 'nuanced', 'detailed', and 'contextual'. Images, videos, voice recordings, finger print and so on, can be considered as qualitative data.

Security with Quantitative data

Quantitative data which is in numerical form is used for security and it is generated by mathematics. There are several types of Mathematical algorithms which convert plaintext(readable) messages into ciphertext(unreadable) messages known as encryption and its reverse process convert ciphertext into plaintext known as decryption. Process of encryption and decryption is known as cryptography. There are several algorithms used in cryptography [2].

Figure 1: The process of encryption and decryption

Cryptography: A cryptosystem is a five-tuple (P, C, K, E, D), where the following conditions are satisfied:

1. P is a finite set of possible plaintexts.
2. C is a finite set of possible ciphertexts.
3. K, the keyspace is a finite set of possible keys.
4. For each $k \in K$, there is an encryption rule $e_k \in E$ and a corresponding decryption rule $d_k \in D$.

Each $e_k : P \to C$ and $d_k : C \to P$ are functions such that $d_k(e_k(x)) = x$ for every plaintext $x \in P$.

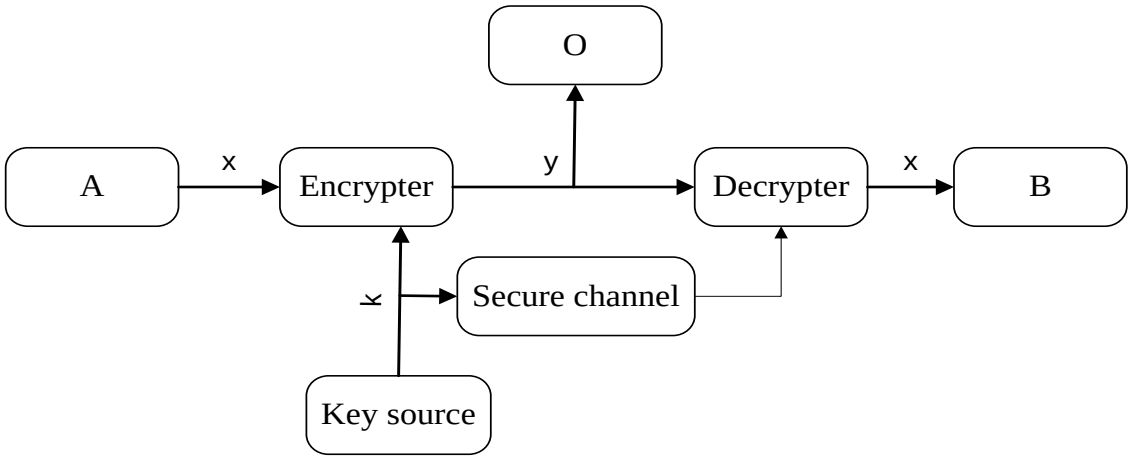

Figure 2: The communication Channel

Login ID and Password:

Generate Up to 500 Random passwords with the ability to determine the composition. For example, you can generate passwords in only uppercase, only lower case, only numbers or any combination of the above. First time person create account with Login Id and corresponding password which are stored in server. Next time whenever person wants to use application, Person is entering their login id and password and after that server verifies it from the server database. If it is verified then person can used their application otherwise not. Hash functions which are the collection of algorithm, are useful for Login id and password.

Key:

In cryptography, a key is a piece of information (a parameter) that determines the functional output of a cryptographic algorithm or cipher. Without a key, the algorithm would have no result. In encryption, a key specifies the particular transformation of plaintext into ciphertext, or vice versa during decryption. Keys are also used in other cryptographic algorithms, such as digital signature schemes and message authentication codes. Random number generators or pseudorandom number generators generate the random key.

The keys can be captured, modified, corrupted, or disclosed to unauthorized persons as the entire operation is dependent upon the security of the keys. In a symmetric cryptosystem, the same key is used for encryption and decryption. In an asymmetric cryptosystem, the key used for decryption is different from the key used for encryption.

The encryption key is known as the public key and the decryption key is known as the private key. The public and private keys are known as a key pair.

RSA Algorithm

The **RSA** algorithm is named after first letter of three computer experts **R**ivest Ron, **S**hamir Adi and **A**dleman Len [3], who invented it in 1977 is playing a vital role in smart card and as well as all e-cards. This algorithm is based on the hard mathematical problem of integer factorization, i.e. given a number which is the product of two large prime numbers; factorize the number to find the primes. Here we see the method to generate the key which is used in encryption and decryption algorithm- parts of RSA algorithm.

Key Generation Algorithm:

1. Generate two large random primes *p* and *q* of approximately equal size such that their product $n = pq$ is of the required bit length, usually of 1024 bits.
2. Compute $n = pq$ and $\phi(n) = (p-1)(q-1)$.
3. Choose an integer *e*, $1 < e < \phi(n)$, such that $\gcd(e, \phi(n)) = 1$.
4. Compute the secret exponent *d*, $1 < d < \phi(n)$, such that $ed \equiv 1 (\mathrm{mod}\ \phi(n))$.
5. The public key is (n, e) and the private key is (n, d). Keep all the values *d*, *p*, *q* and $\phi(n)$ secret.

Here *n*, *e*, *d* are known as the *modulus*, *exponent* and *decryption* exponent respectively. After the generation of key, the plaintext can be encrypted and decrypted as follows:

Encryption: Sender A wants to send a message M $[\mathbf{M} < \mathbf{n}]$ to B. To encrypt the message the following procedure is adopted.

$$M = M^e$$ where *e* is the B's public-key.

1. Compute the integer remainder when M^e is divided by *n* [B's modulus for encryption and decryption].
2. Represents the plaintext message as a positive integer $M(< n)$.
3. Computes the ciphertext $C \equiv M^e \pmod n$.
4. Sends the ciphertext C to B.

Decryption: Recipient B does the following:

1. Uses his private key (n, d) to compute $M \equiv C^d \pmod n$.
2. Extracts the plaintext from the message representative *M*.

Here we present a simple example of the RSA algorithm. This example was considered by Singh [4]. For this example, the key were generated as follows:

1. Select two prime numbers, p = 17 and $q = 11$.
2. Calculate $n = pq = 17 \times 11 = 187$.
3. Calculate $\phi(n) = (p-1) \times (q-1) = 16 \times 10 = 160$.
4. Select *e* (=7) such that *e* is relatively prime to $\phi(n) = 160$ and less than $\phi(n)$. Determine *d* such that $de \equiv 1 \pmod{160}$ and $d < 160$.

Find *d* such that $7d \equiv 1 \pmod{160}$. We get $d = 23$, since $23 \times 7 = 161$.

The resulting keys are public key $KU = (7, 187)$ and private key $KR = (23, 187)$. The example shows the use of these keys for a plaintext input of $M = 88$.

Encryption: Calculate C such that $C \equiv M^e \pmod n$,

$$\therefore C \equiv 88^7 \equiv 88^4 \times 88^2 \times 88^1 \equiv 8,94,432 \equiv 11 \pmod{187}.$$

Decryption: Calculate $M \equiv C^d \pmod n$

$$\therefore M \equiv 11^{23} \equiv (11^1) \times (11^2) \times (11^4) \times (11^8) \times (11^8) \equiv 79720245 \equiv 88 \pmod{187}.$$

The above example can be summarized as shown below:

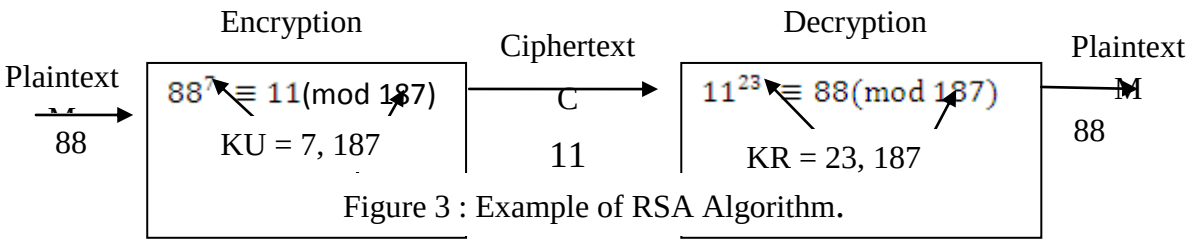

Figure 3 : Example of RSA Algorithm.

Authentication using Smart Card Technology:

While using the smart card and entered the password, the smart card reader will first confirm (authenticate) the password. The following figure shows the use of RSA algorithm in PKC.

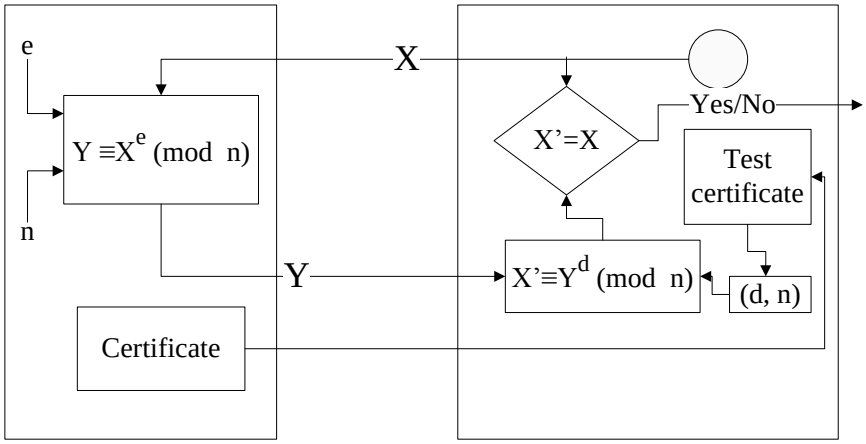

Figure 4: Public Key Authentication using RSA algorithm

The following is the list of characters which is used in above figure.

X = Random challenge to Smart card
Y= Cipher text
e = Encryption exponent
d = Decryption exponent
X' = Random challenge number.
n = modulus

Here is the example of authentication of smart card using private and public key. First the server sends a random challenge say $X = 9726$ to smart card. Further suppose that the value $(e, n) = (3533, 11413)$ is provided by the smart card to the server. Now the value of Y is calculated as follows:

$$Y \equiv X^e \pmod{n} \equiv 9726^{3533} \pmod{11413} \equiv 5761 \pmod{11413}.$$

So the values $(e, n) = (3533, 11413)$ and $Y = 5761$ is sent back by the card to the server along with the password (say)$p = 101$. Then the server immediately calculates the value of *q* by the result $n = pq$. Here $n = 11413$ and $p = 101$, which gives the value $q = 113$.

Next server needs to calculate the value of *d*, for which it needs to calculate the value of $\phi(n)$ using the relation $\phi(n) = (p-1) \times (q-1)$.

Here $\phi(n) = (101-1) \times (113-1) = 100 \times 112 = 11200 = 2^6 \times 5^2 \times 7$ and

$$\gcd(e, \phi(n)) = \gcd(3533, 11200) = 1.$$

Thus the linear congruence $ed \equiv 1 \pmod{\phi(n)}$ is solvable.

$$\therefore d \equiv e^{-1} \pmod{\phi(n)} \equiv 3533^{-1} \pmod{11200} \equiv 6597 \pmod{11200}.$$

Hence the public-key is $(d, n) = (6597, 11200)$ and noted that $\gcd(d, n) = \gcd(6597, 11200) = 1$.

Finally the value X' is calculated by the relation $X' \equiv Y^d \pmod{n}$. Therefore we get

$$X' \equiv Y^d \equiv 5761^{6597} \equiv 9726 \pmod{11413}.$$

This gives $X' = 9726$. Hence $X' = X$. Thus the digital signature is verified and the smart card can now be accessed. In RSA algorithm, is useful for verify the human quantitative data, which is stored in memory of server. The RSA algorithm is currently used in secure telephones, Ethernet network cards, smart cards, credit card, debit card and

master card and at many more places. It is also used internally in many institutions, including branches of the U.S. government, major corporations, national laboratories and universities.

Security with Qualitative data

The word "biometrics" is derived from the Greek words 'bios' means life and 'metric' means measurement. This directly translates into "life measurement". There are basically two types of biometrics Behavioral Biometrics and Physical Biometrics. Behavioral biometrics measures the characteristics which are acquired naturally over a time. It is generally used for verification. Speaker Recognition, Signature, Keystroke are the examples of behavioral biometric. Physical biometrics measures the inherent physical characteristics on an individual. It can be used for either identification or verification. Fingerprint, Facial Recognition, Hand Geometry, Iris Scan, Retinal Scan, Vascular Patterns, DNA etc... are the examples of physical biometric. Total security system is identifies and verifies both types of data quantitative and qualitative of human [6].

There are two different ways to resolve a person's identity: Verification (*or one-to-one-processing*) and Identification (*or one-to-many-processing*). Verification (*Am I whom I claim I am?)* involves confirming or denying a person's claimed identity. In identification, one has to establish a person's identity (*Who am I?*). Each one of these approaches has its own complexities and could probably be solved best by a certain biometric system [8].

There are seven types of biometric measurements- Face recognition Fingerprint recognition, Hand geometry, Retinal scanners, Iris recognition, voice recognition are commonly used today for security. These are work with the most obvious individual identifier of the human. This recognition system analysis the characteristics of person based on input image, system measures the characteristic of human including distances between eyes, nose, mouth, chicks, fingerprint, hand geometry etc. With the use of above unique characteristics, recognition system store human template into its database [1].

Mathematical technique for Image verification

In statistics, principal components analysis (PCA) is a technique that can be used to simplify a dataset. PCA is also based on an information theory approach that decomposes images into small set of feature images called "Eigenimages" which may be thought of as principle component analysis of original training set of human images. The algorithm of this method (PCA) is described as follows [5]:

Step 1: Establishes the training set.

The first step is to obtain a set S with M images. Each image is transformed into a vector of size N and placed into the set.

$$S = \{a_1, a_2, a_3, \dots, a_M\}$$

Step 2: Calculate the mean.

The mean image μ from the set S is $\mu = \frac{1}{M}\sum_{i=1}^{M} a_i$

Step 3: Subtract the mean from original image.

Calculate the difference between the input image and the mean image and the result is stored in Φ.

$$\Phi_i = a_i - \mu$$

Step 4: Calculate the covariance matrix.

The covariance matrix C is calculated in the following manner

$$C = \frac{1}{M}\sum_{n=1}^{M} \Phi_n \Phi_n{}^T = AA^T \quad \text{where } A = \{\Phi_1, \Phi_2, \Phi_3, \dots, \Phi_n\}$$

Step 5: Calculate the eigenvectors and eigenvalues of the covariance matrix and select the principal components.

Calculate the eigenvectors of the covariance matrix C has dimension $N^2 \times N^2$. For images of a significant size this is a large computational task. We can solve for N^2 dimensional eigenvectors in this case by first solving the Eigen vectors of $n \times n$ matrix. i.e. AA^T

$$(AA^T)V_i = \lambda_i V_i$$
$$A(A^T A)V_i = A(\lambda_i V_i)$$
$$(AA^T)(AV_i) = \lambda_i (AV_i)$$

Where V_i and λ_i are eigenvectors and eigenvalues of the smaller $(n \times n) A^T A$ matrix respectively. The eigenvector of the larger AA^T matrix can be computed by calculating AV_i the eigenvectors are stored in descending order of eigenvalues. They are shown in below:

$$U_i = AV_i = [\Phi_1, \Phi_2, \Phi_3, \dots, \Phi_n] * \begin{pmatrix} v_1{}^i \\ \cdot \\ v_k{}^i \\ \cdot \\ v_n{}^i \end{pmatrix} = \sum_{k=1}^{n} v_k{}^i \Phi_k$$

Training set Eigen image

Figure 5: Eigen Image has a Image like appearance

Here eigenimages are determined; the "training" phase of the algorithm is finished. Once the training set has been prepared the next phase is the classification of new input images.

Step 6: Transform the new image

The new image is transformed into its eigenimage components using following computation

$$W_i = U_i{}^T (a - \mu)$$

where $W = \text{weight vector}$, $a = \text{new input image}$, $\mu = \text{mean image}$. Each value would be represent a weight and would be saved on a vector Ω. The weight vector Ω^T is given by,

$$\Omega^T = [W_1, W_2, \dots, W_M]$$

Step 7: Calculate Euclidean Distance

We now determine which image class provides the best description for the input image. This is done by minimizing the Euclidean distance

$$\varepsilon_k = ||\Omega - \Omega_k||^2$$

The input image is consider to belong to a class if ε_k is bellow an established threshold θ_ε. Then the human image is considered to be a known image. If the difference is above the given threshold, but bellow a second threshold, the image can be determined as an unknown image. If the input image is above these two thresholds, the image is determined NOT to be a image. If the image is found to be an unknown image, you could decide whether or not you want to add the image to your training set for future recognitions. You would have to repeat steps 1 trough 7 to incorporate this new image.

Flow chart:

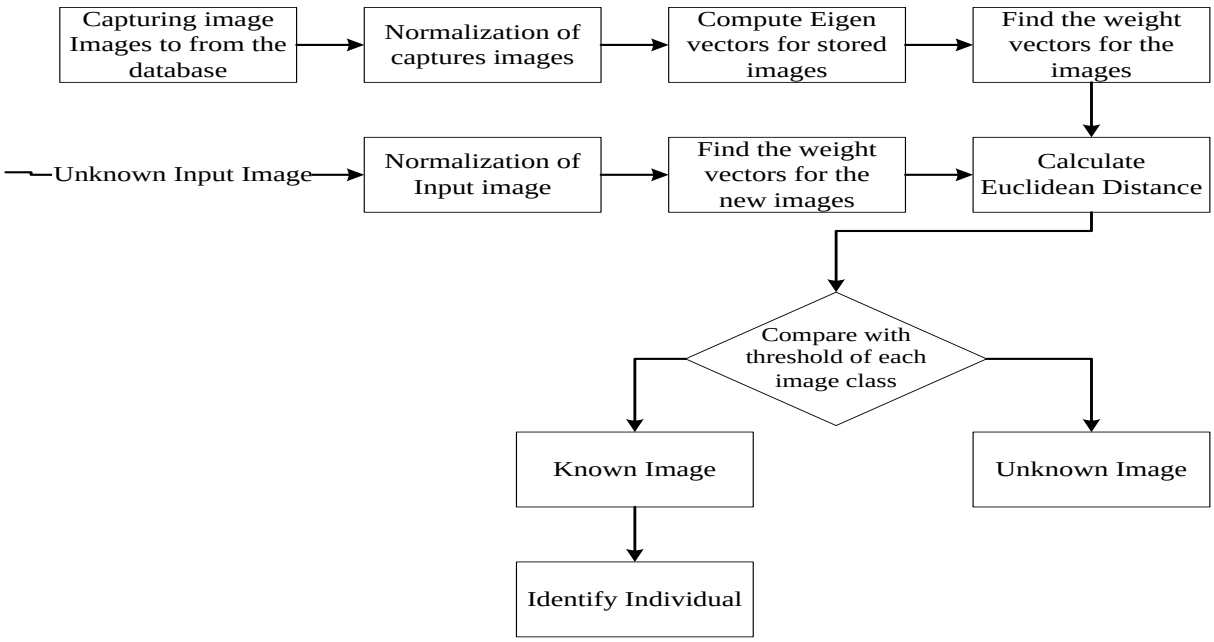

Figure 6: Architectural Flow Diagram for Recognition using PCA

As shown in above Figure, first the original images of the training set are transformed into a set of eigenimages. Afterwards, the weights are calculated for each image of the training set and stored. Upon observing an unknown image X, the weights are calculated for that particular image and stored in another vector. Afterwards, the weight vector of the new image is compared with the weights of the stored images. This is done by considering each weight vector as a point in space and calculating the average distance *d* between the weight vectors (vector of the unknown image and that of the stored images) which is then compared with a threshold value to decide upon whether it is a known or unknown image.

In this algorithm, the image classified by Neural Network it is matched by the system with all the image sequence of characteristics. Here, system finds the association between stored group of image and classified image. After compression the highly associated images will be displayed. At this level it is important to discuss that the human image may consist the characteristics of more than one images or it's a combination. In this case image is matched with all the groups of Images and displayed that Images whose proportion of characteristics is more matched compare to other with image. So with this procedure we can easily find the characteristics with images.

Conclusion

The total security system works with qualitative data and quantitative data of human and identifies human characteristics, which is highly beneficial for Bank, Military, Crime branch etc.

References

[1] Albert M., Biometrics unique and diverse applications in nature, science and technology, InTech, 2011.

[2] Stinson D. R., Cryptography Theory and Practice, CRC Press, Inc. 1995.

[3] Rivest R. L., Shamir A. and Adleman L.,A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, Vol.21,1978, 120-126.

[4] Singh S., The code Book : The Science of secrecy from Ancient Egypt to Quantum Cryptography, New York , Anchor Books, 1999.

[5] Turk, M., and Pentland, A., "Eigenfaces for recognition", Journal of Cognitive Neuroscience, Vol. 3, pp. 71-86, (1991).

[6] Yang J., Biometrics, InTech,2011.

[7] http://www.socialresearchmethods.net/kb/datatype.php

[8] http://biometrics.cse.msu.edu/info.html