Enhanced Cryptography Technique: By Integrating Color and Arm Strong Numbers for Data Transfer

N.Akhila [#1], D.Sowmya Sree[*2], K.Praveen Kumar[*3]

Assistant Professor [#1], Senior Lecturer[*2], Java Developer [*3]

Department of Computer Science & Engineering,
GIET College, NH-16, Rajahmundry
East Godavari (District), AP (INDIA).

Abstract

Security is the degree of resistance to, or protection from, harm. It applies to any vulnerable and valuable asset, such as a person, dwelling, community, nation, network or organization. In real time environment, data security plays a vital role where the following factors like confidentiality, authentication, integrity, non-repudiation have given a high importance. We clearly know that cryptography is a major technique for providing confidentiality for the transmitted data through some network media. In this paper we have implemented a new technique to encrypt the data using a key involving Armstrong numbers and colors as the two level password. Three set of keys are used to provide secure data transmission with the colors acting as vital security element thereby providing authentication for the storage data. By performing various experiments on the proposed method, our simulation results on various types of storage data clearly tells that our proposed technique is having high level of security when compared with existing cryptography algorithms.

Keywords

Cryptography, Security, Armstrong, Non-Repudiation.

1. Introduction

Information security, sometimes shortened to **InfoSec**, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (electronic, physical, etc[7].

Sometimes information security is also referred to be as computer security, Information Technology Security is information security applied to technology (most often some form of computer system). It is worthwhile to note that a computer does not necessarily mean a home desktop. A computer is any device with a processor and some memory. Such devices can range from non-networked standalone devices as simple as calculators, to networked mobile computing devices such as smartphones and tablet computers. IT security specialists are almost always found in any major enterprise/establishment due to the nature and value of the data within larger businesses. They are responsible for keeping all of the technology within the company secure from malicious cyber-attacks that often attempt to breach into critical private information or gain control of the internal systems.

In the present world scenario it is difficult to transmit data from one place to another with

security. This is because hackers are becoming more powerful nowadays. To ensure secured data transmission there are several techniques being followed. One among them is cryptography which is the practice and study of hiding information

2. Background Theory

In this section we will describe the background work and assumptions that are used in the proposed paper.

Data Security Technologies

Some of the information security based technologies are as follows. As security plays a vital role in transmitting of data through either wired or wireless channel. There are several mechanisms for providing security for the data; some of them are as follows:

2.1 Disk Encryption Mechanism

Disk encryption refers to encryption technology that encrypts data on a hard disk drive. Disk encryption typically takes form in either software (see disk encryption software) or hardware (see disk encryption hardware). Disk encryption is often referred to as on-the-fly encryption (OTFE) or transparent encryption.

2.2 Hardware-Based Mechanisms for Protecting Data

Software-based security solutions encrypt the data to prevent it from theft. However, a malicious program or a hacker could corrupt the data in order to make it unrecoverable, making the system unusable. Hardware-based security solutions can prevent read and write access to data and hence offer very strong protection against tampering and unauthorized access.

Hardware-based or assisted computer security offers an alternative to software-only computer security. Security tokens such as those using PKCS#11 may be more secure due to the physical access required in order to be compromised. Access is enabled only when the token is connected and correct PIN is entered (see two-factor authentication). However, dongles can be used by anyone who can gain physical access to it. Newer technologies in hardware-based security solves this problem offering fool proof security for data.

Working of hardware-based security: A hardware device allows a user to log in, log out and set different privilege levels by doing manual actions. The device uses biometric technology to prevent malicious users from logging in, logging out, and changing privilege levels. The current state of a user of the device is read by controllers in peripheral devices such as hard disks. Illegal access by a malicious user or a malicious program is interrupted based on the current state of a user by hard disk and DVD controllers making illegal access to data impossible. Hardware-based access control is more secure than protection provided by the operating systems as operating systems are vulnerable to malicious attacks by viruses and hackers. The data on hard disks can be corrupted after a malicious access is obtained. With hardware-based protection, software cannot manipulate the user privilege levels. It is impossible for a hacker or a malicious program to gain access to secure data protected by hardware or perform unauthorized privileged operations. This assumption is broken only if the hardware itself is malicious or contains a backdoor.[2] The hardware protects the operating system image and file system privileges from being tampered. Therefore, a completely secure system can be created using a combination of hardware-based security and secure system administration policies.

2.3 Data Masking Mechanism

Data Masking of structured data is the process of obscuring (masking) specific data within a database table or cell to ensure that data security is maintained and sensitive information is not exposed to unauthorized personnel. This may include masking the data from users (for example so banking customer representatives can only see the

last 4 digits of a customer's national identity number), developers (who need real production data to test new software releases but should not be able to see sensitive financial data), outsourcing vendors, etc.

2.4 Data Erasure Mechanism

Data erasure is a method of software-based overwriting that completely destroys all electronic data residing on a hard drive or other digital media to ensure that no sensitive data is leaked when an asset is retired or reused.

3. Cryptography

Cryptography, to most people, is concerned with keeping communications private. Encryption is the transformation of data into some unreadable form. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended. Decryption is the reverse of encryption; it is the transformation of encrypted data back into some intelligible form.

Encryption and decryption require the use of some secret information, usually referred to as a key. The data to be encrypted is called as plain text. The encrypted data obtained as a result of encryption process is called as cipher text. Depending on the encryption mechanism used, the same key might be used for both encryption and decryption, while for other mechanisms, the keys used for encryption and decryption might be different.

3.1 Types of Cryptographic Algorithms

There are several ways of classifying cryptographic algorithms. In general they are categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use as in **[1].** The three types of algorithms are depicted as follows

1) **Secret Key Cryptography (SKC):** Uses a single key for both encryption and decryption. The most common algorithms in use include Data Encryption Standard (DES), Advanced Encryption Standard (AES).

2) **Public Key Cryptography (PKC):** Uses one key for encryption and another for decryption. RSA (Rivest, Shamir, Adleman) algorithm is an example.

3) **Hash Functions:** Uses a mathematical transformation to irreversibly "encrypt" information. MD (Message Digest) algorithm is an example.

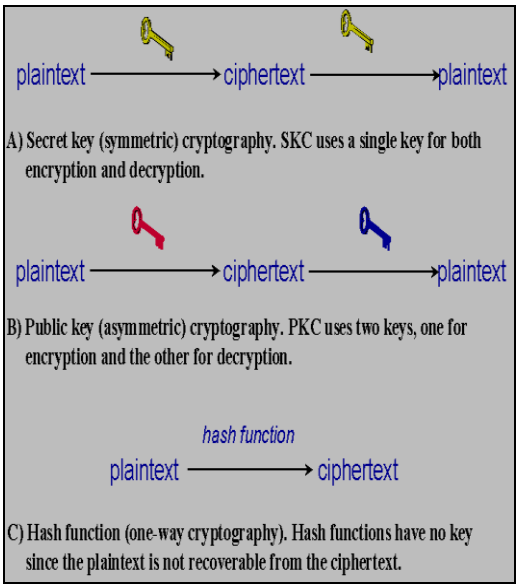

Fig. 1 Represents various types of Cryptographic Algorithms

4. Proposed Methodologies

The following are the various methodologies that are used in the proposed paper. They are as follows:

4.1 RGB Color Model

Any color is the combination of three primary colors Red, Green and Blue in fixed quantities. A color is stored in a computer in form of three numbers representing the quantities of Red, Green and Blue respectively. This representation is called RGB representation which is used in computers to store images in BMP, JPEG and PDF formats. Here each pixel is represented as values for Red, Green and Blue. Thus any color can be uniquely represented in the three dimensional RGB cube as values of Red, Green and Blue.

The RGB color model is an additive model in which Red, Green and Blue are combined in various ways to produce other colors. By using appropriate combination of Red, Green and Blue intensities, many colors can be represented. Typically, 24 bits are used to store a color pixel. This is usually apportioned with 8 bits each for red, green and blue, giving a range of 256 possible values, or intensities, for each hue. With this system, 16 777 216 (256^ 3 or 2^24) discrete combinations of hue and intensity can be specified.

4.2 Integration of Color and Arm Strong Number

The existing techniques involve the use of keys involving prime numbers and the like. As a step further ahead let us considers a technique in which we use Armstrong numbers and colors. Further we also use a combination of substitution and permutation methods to ensure data security.

We perform the substitution process by assigning the ASCII equivalent to the characters. Permutation process is performed by using matrices as in [2] and Armstrong number. In this technique the first step is to assign a unique color for each receiver. Each color is represented with a set of three values. For example violet red color is represented in RGB format as (238, 58,140). The next step is to assign a set of three key values to each receiver as shown in figure 2.

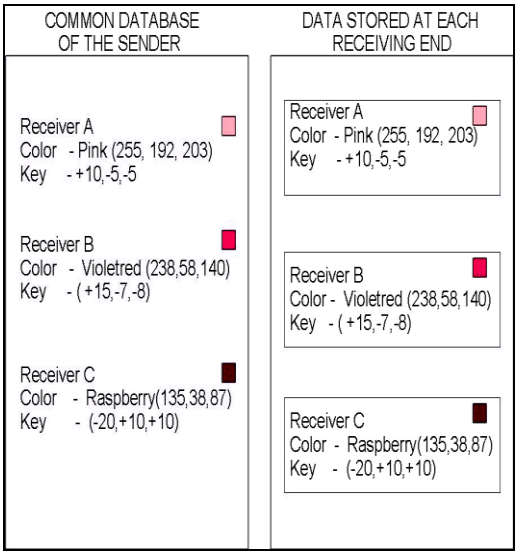

Figure. 2: Represents Data at Sender and Receiver Side.

The sender is aware of the required receiver to whom the data has to be sent. So the receiver's unique color is used as the password. The set of three key values are added to the original color values and encrypted at the sender's side. This encrypted color actually acts as a password. The actual data is encrypted using Armstrong numbers. At the receiver's side, the receiver is aware of his own color and other key values. The encrypted color from the sender is decrypted by subtracting the key values from the received set of color values. It is then tested for a match with the color stored at the sender's database. Only when the colors are matched the actual data can be decrypted using Armstrong numbers. Usage of colors as a password in this way ensures more security to the data providing authentication[4]. This is because only when the colors at the sender and receiver's side match with each other the actual data could be accessed[5].

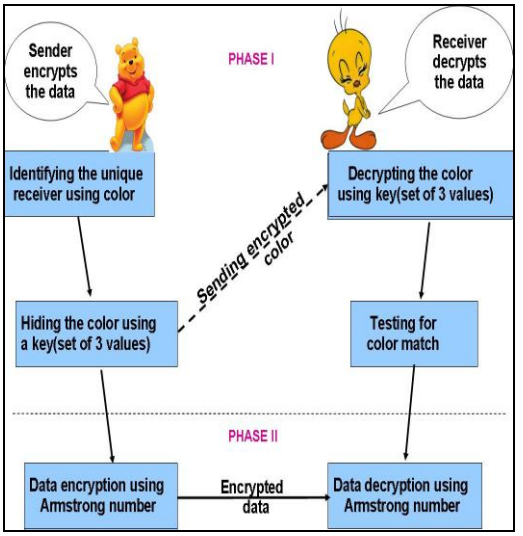

Figure. 3 Represents the Proposed Integration Techniques

Example

1) **Encryption:** As an illustration let us assume that the data has to be sent to a receiver (say A) who is assigned the color raspberry (135, 38, 87). Let the key values to be added with this color value be (-10, +5, +5). Let the Armstrong number used for data encryption be 153.

Step 1: (Creating Password)

Initially the sender knows the required receiver to be A. So the key values are added with the color values assigned for receiver A.

135 38 87

-10 5 5

---

125 43 92

Now a newly encrypted color is designed for security check.

Step 2: (Encryption of the actual data begins here)

Let the message to be transmitted be "CRYPTOGRAPHY".

First find the ASCII equivalent of the above characters.

C	**R**	**Y**	**P**	**T**	**O**	**G**	**R**	**A**	**P**	**H**	**Y**
67	**82**	**89**	**80**	**84**	**79**	**71**	**82**	**65**	**80**	**72**	**89**

Step 3: Now add these numbers with the digits of the Armstrong number as follows

67 82 89 80 84 79 71 82 65 80 72 89
(+)1 5 3 1 25 9 1 125 27 1 5 3
---
68 87 92 81 109 88 72 207 92 81 77 92

Step 4: Convert the above data into a matrix as follows

A=

$$\begin{bmatrix} 68 & 81 & 72 & 81 \\ 87 & 109 & 207 & 77 \\ 92 & 88 & 92 & 92 \end{bmatrix}$$

Step 5: Consider an encoding matrix...

B =

$$\begin{bmatrix} 1 & 5 & 3 \\ 1 & 25 & 9 \\ 1 & 125 & 27 \end{bmatrix}$$

Step 6: After multiplying the two matrices (B X A) we get

C =

$$\begin{bmatrix} 779 & 890 & 1383 & 742 \\ 3071 & 3598 & 6075 & 2834 \\ 13427 & 16082 & 28431 & 12190 \end{bmatrix}$$

The encrypted data is...

779, 3071, 13427, 890, 3598, 16082, 1383, 6075, 28431, 742, 2834, 12190

The above values represent the encrypted form of the given message.

2) Decryption

Decryption involves the process of getting back the original data using decryption key. The data given by the receiver (the color) is matched [6] with the data stored at the sender's end. For this process the receiver must be aware of his own color being assigned and the key values.

Step 1: (Authenticating the receiver)

For the receiver A (as assumed) the actual color being assigned is Raspberry. (135, 38, 87), the key values (set of three values) are subtracted from the color being received to get back the original color.

The decryption is as follows.

```
    125  43   92 (Received data)
(-) -10   5    5 (Key values)
---------------------------------
    135  38   87
```

The above set of values (135, 38, 87) is compared with the data stored at the sender's side. Only when they both match the following steps could be performed to decrypt the original data.

Step 2 :(Decryption of the original data begins here)

The inverse of the encoding matrix is

$$D = (-1/240) * \begin{bmatrix} -450 & 240 & -30 \\ -18 & 24 & -6 \\ 100 & -120 & 20 \end{bmatrix}$$

Step 3: Multiply the decoding matrix with the encrypted data

$$\begin{bmatrix} 68 & 81 & 72 & 81 \\ 87 & 109 & 207 & 77 \\ 92 & 88 & 92 & 92 \end{bmatrix}$$

(D X C) we get

Step 4: Now transform the above result as given below

68 87 92 81 109 88 72 207 92 81 77 92

Step 5: Subtract with the digits of the Armstrong numbers as follows

```
  68 87 92 81 109 88 72 207 92 81 77 92
(-)1  5  3  1   25  9  1 125 27  1  5  3
-----------------------------------------------------
  67 82 89 80 84 79 71 82 65 80 72 89
```

Step 6: Obtain the characters from the above ASCII Equivalent

```
67 82 89 80 84 79 71 82 65 80 72  89
C  R  Y  P  T  O  G  R  A  P  H  Y
```

5. Implementation Modules

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods. The proposed consists of totally four modules:

5.1 User Authentication Module

In this technique, we use RGB color model for user authentication, were a discrete and unique set of

colors, i.e., 16 777 216 (256^ 3) combinations of colors can be defined. The sender assigns unique color for each user and this detail is stored in a database. The sender is aware of the required receiver to whom the data has to be sent. A set of three key values are added to the original color values and encrypted at the sender's side. This encrypted color actually acts as a password. The sender sends the key value to the receiver. The receiver is aware of the color assigned to him. The receiver decrypts the color by subtracting the key values from the encrypted color values. If the decrypted color value matches with the color value stored in the database, then the user is an authenticated user. Usage of colors helps to enhance security of data; this is because only if the color at receiver side matches the color on the sender side, original data can be accessed.

5.2 Data Encryption Module:

Once the user is authenticated, now the sender sends the requested data to the receiver. Initially ASCII value for each character is found. Then Armstrong number is added to this ASCII value in an iterative manner until each character is assigned with the number. The resultant sum value is now converted into a matrix. Consider an encrypted matrix (Armstrong number), multiply it with the resultant sum matrix. The resultant matrix value consists of the encrypted data.

5.3 Receiver Module:

The receiver of this module will receive encrypted code and they have to decrypt it also to decrypt a message.

5.4 Data Decryption Module

The data which is encrypted and hidden is received at the receiver side. The data is extracted now. The inverse of the encoding matrix (Armstrong number) is found, and it is the decoding matrix. On receiving the encrypted data, the data is rearranged to the original order, which is gives the correct order of the encrypted data. Now this data is arranged in matrix format and it is multiplied with the decoding matrix. The resultant value gives the ASCII value of the characters. Thus the data is decrypted and original data is got back.

6. Conclusion

In this paper, we proposed a new integration of color and Arm strong number technique for providing high level of security for the data centers which communication large amount of data.The above combination of secret key and public key cryptography can be applied mainly in military where data security is given more importance. This technique provides more security with increase in key length of the Armstrong numbers. Thus usage of three set of keys namely colors, additional set of key values and Armstrong numbers in this technique ensures that the data is transmitted securely and accessed only by authorized people.

7. References

[1] Atul Kahate, "Cryptography and Network Security ", Tata McGraw Hill Publications.

[2] ttp://aix1.uottawa.ca/~jkhoury/cryptography.htm

[3] http://www.scribd.com/doc/29422982/Data-Compression-and-Encoding-Using-Col.

[4] Summers, G. (2004). Data and databases. In: Koehne, H Developing Databases with Access: Nelson Australia Pty Limited. p4-5.

[5] Waksman, Adam; Sethumadhavan, Simha (2011), "Silencing Hardware Backdoors", *Proceedings of the IEEE Symposium on Security and Privacy* (Oakland, California).

[6] Peter Fleischer, Jane Horvath, Shuman Ghosemajumder (2008). "Celebrating data privacy". Google Blog. Retrieved 12 August 2011.

[7] Cherdantseva Y. and Hilton J.: Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals. In: Organizational, Legal, and Technological Dimensions of Information System Administrator. Almeida F., Portela, I. (eds.). IGI Global Publishing. (2013).

8. About the Authors

N.Akhila is currently working as Assistant Professor, in Department of Computer Science and Engineering at GIET College, Rajahmundry, East Godavari District, India. She completed her M.Tech in CSE at GIET College of Engineering in the month of Dec 2012. Her research interests include Networks Security, Information Security and Data Mining.

.

D.Sowmya Sree is currently working as Senior Lecturer, in Department of Computer Science at Sri Chaitanya Junior College for CBSE Girls campus, Kommadi, Visakhapatnam. She completed her M.Tech in CSE at Chaitanya Engineering College, Kommadi in the month of Dec 2012.Her research interests include Networks Security, Information Security, Data Mining, and Computer Programming in Java.

K. Praveen Kumar is currently working as Java Team Leader in Genisys Technologies, MVP sector 6, Visakhapatnam. He completed his M.Tech in CSE at Chaitanya Engineering College, Kommadi in the month of Dec 2012.His research interests include Networks Security, Information Security, Data Mining, Image Processing and Computer Programming in Java.