American Journal of Applied Mathematics
2015; 3(1-2): 1-8
Published online December 26, 2014 (http://www.sciencepublishinggroup.com/j/ajam)
doi: 10.11648/j.ajam.s.2015030102.11
ISSN: 2330-0043 (Print); ISSN: 2330-006X (Online)

Public cloud user authentication and data confidentiality using image steganography with hash function

Bidisha Goswami*, Ravichandra G.

Computer Science & Engineering, PES Institute of Technology, Bangalore South Campus, Bangalore, India

Email address:
bidishagoswami@pes.edu (B. Goswami), bhoomimoon@gmail.com (Ravichandra G.)

To cite this article:
Bidisha Goswami, Ravichandra G.. Public Cloud User Authentication and Data Confidentiality Using Image Steganography with Hash Function. *American Journal of Applied Mathematics.* Special Issue: Frontiers in Mathematics and Computing.
Vol. 3, No. 1-2, 2015, pp. 1-8. doi: 10.11648/j.ajam.s.2015030102.11

Abstract: Public cloud is an environment in which many users share resources, but the consumer has to sacrifice security owing to the multi - tenancy feature of cloud computing. However, maintaining Confidentiality and Security for critical data is highly challenging. Taking account of the static nature of user validation, this paper address authentication and confidentiality issues. A methodology has been proposed for user authentication to make cloud server, dynamic in nature, based on the time stamp and other parameters. The confidential data are embedded randomly in images using steganography as a basic technique, in which a new method of encryption and decryption is proposed. The methodology of encryption or decryption uses odd Fibonacci series values and a hash function to prepare hash value series. This hash value series is multiplied with ASCII codes of the original data which need to embed, in decryption process and similar technique have been used here, rather than the technique of multiplying ASCII codes with hash value using division operation.

Keywords: Privacy, Cloud computing, Steganography, Encryption, Decryption, Hash Function

1. Introduction

This paper interprets the data security and privacy issues in a public cloud environment. Cloud computing technology provides storage as a service to all kinds of clients; however, there are two main concerns in the form of security and privacy of data during adaptation of cloud. There are some extremely sensitive data such as health records, account details and company confidential matters. These data need more security and confidentiality with special attention [1].This paper addresses these concerns by highlighting a new methodology of data encryption and user authentication. A mature data encryption implies the confidentiality and secrecy of data. The nature of cloud is highly volatile and dynamic. This proposition makes it even more challenging for the existing encryption techniques to fulfill all enforcements of organizational standard. The paper [9] explains how confidential data like personal health records, bank accounts details, and other secret data of end users need more protection against hackers [9]. There is an existing privacy law called HIPPA (Health Insurance Probability and Accountability Act) which details about security issues involving health records. They commonly treat these records in a way that it should not transform into a cloud [6]. This paper tried to propose a security model for medical heath record security issues which would work for the health record transaction.

Different companies offer to provide cloud services like SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service), etc. They place user critical data on cloud storage space, which plays a big role against the insecurity of public clouds. These companies or cloud service providers are tied up with Life Insurance Companies (LIC) or Government [7]. Sometimes critical data like health records, if hacked, may pose as a threat to patient privacy. It is a new challenge how to store critical data like patient record which need to be transmitted frequently in multi-tenanted platforms like a cloud, grid, etc. Hence public cloud storages need secure and reliable encryption mechanisms to hold critical data on it. In traditional privacy encryption mechanisms, for example, Attribute Based Encryption (ABE) [8] uses identity information such as SSN, name, passport details, etc., however, the likes of crypt analyzer will easily break this

kind of cipher-text into plain text if it is able to guess personal attributes of the sender [10].

Image encryption technique or steganography possess different types of embedding schemes, in which LSB method is achieved by eliminating least significant bit of image binary value of the secret data byte [14]. Accessing confidential data can obtained applying blind method of elevating each LSB bit. There has been some work done on transformation of image pixels based on certain criteria, which says how much confidential data is going to be twisted to enforce the encryption.

The proposed system in this paper address embedded confidential data in an image in a similar way of image steganography, but here a random method is used to choose pixel values or grayscale in which confidential data is going to be hidden. Before hiding the data on the cover image, a method of confidentiality converts each character into its equivalent ASCII codes and then multiply them with hash values. The hash value is generated using a hash function, and it takes odd Fibonacci series as input and hash value becomes the output. The proposed paper use four twists, which are used for hiding data in cover image.

The rest of the paper is organized as follows. Part II describes in detail about proposed system components used to build our system. Example depicting conversion of plain text to cipher text conversion is described in part III. The system architecture is described in part IV. Part V describes cloud server authentication. Part VI describes highly efficient factors, i.e., trade-off security analysis over existing cloud security systems of the proposed system. Final Part VII concludes the overall paper and part VIII provide references related to our work.

2. Proposed System Component

To facilitate our discussion of system components, at first Public Cloud User Authentication and Data Confidentiality is established through Image steganography. A Hash Function is embedded with this steganograpy technique. It consists of four components: The cloud service provider (CSP) who provides all resources of cloud to end user with some arbitrary recommendations. It provides storage as a service in a public cloud. This component encrypts critical data of end users and stores on a cloud server. CSP delivers the secret key to end user for decrypt of cipher texts present in cloud server. Individual clients collect their personal data from cloud server, encrypt the private key from CSP and then decrypt it. The second component is cloud server which stores all confidential information and maintains a log report for every file present in it. It provides different aspects for the client to understand their data stored in cloud server. The third part is a user or a client for CSP having a valid PID, Password and mobile ID (MID) who will record the inside information and obtain admittance to the confidential data stored in cloud server. Fourth component is Trusted Party Authority (TPA) which is responsible for identifying cloud servers and user authentication. It gets a token based on user request and then doling out the tokens (i.e., private keys) to the individual clients and the cloud server. The cloud server matches both the keys during data request from private users. The TPA collects the service fee from the users according to a certain payment model, known pay-as-you-go payment model.

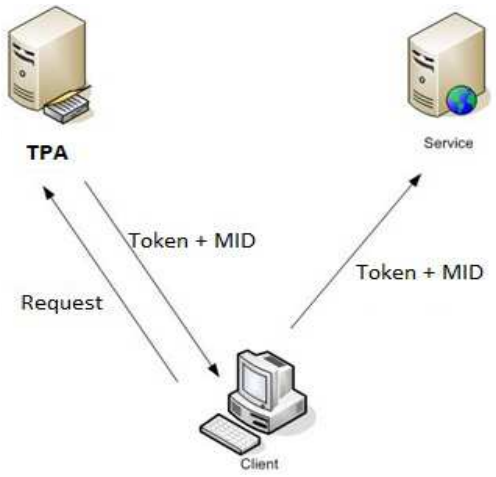

Fig. 1. *User authentication in cloud*

Cloud user authentication is fairly easy to achieve, because of the static nature of user validation as existing cloud authentication consist of cloud id and password only. This paper addresses the static nature of user validations, so and paves its way into dynamic validation. End user request TPA for granting token for accessing particular cloud server. This request contains a user name, password, system IP address and time stamp. After receiving requests from end users, TPA validates user name and password and it generates token for the end user. With this ticket, TPA issues a mobile id (MID). MID generation is based on the TPA server system environment, therefore is not redundant. The Cloud server verifies username, password MID and token of a particular user login with respect to system parameter.

The proposed encryption algorithm is based on image steganography and hash function cryptography techniques to maintain the confidentiality of data stored in the cloud. Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated. The strength of steganography can thus be amplified by combining it with cryptography. The proposed system uses a combination of image stenography and hash cryptography techniques.

The confidential data are embedded randomly in images using steganography as a basic technique in which a new method of encryption and decryption is proposed . Fibonacci series is a wonderful technique for problem solving. The specialty of this technique is used in encryption and

decryption. The proposed methodology uses odd Fibonacci series values, i.e. by eliminating every third even number with masked value. These values are provided to hash function as input values; and the final result is a hash value. This hash value series is multiplied with ASCII codes of the original data which is embedded in decryption process. Now to incorporate these multiplied value on cover image a random pixel gray scale value is chosen. The same technique is used for generation of hash value series on the client side, where it is used instead of multiplying ASCII codes with hash value use division operation. The decryption process is opposite of the encryption process with required key. This is described in detail in part IV of this paper.

Module Description: Architecture of Public Cloud User Authentication and Data Confidentiality Using Image Stegnography with Hash Function mainly consists of five modules which are described as follows:

Module 1: User Module- Individual users, collect their data from cloud server, decrypt it, and then store in their mobile devices. Decryption is done at the user side, so secret key which is necessary for decryption is sent from CSP to the user.

- User module contains a username, password and MID (Mobile ID) which is received by the end user through SMS.
- The user sends a request to the TPA for connection to a valid server and trigger the authentication process
- Download encrypted cover image from cloud server into user system.
- The secret key is issued by CSP to the user in a secured manner.
- Call data_decryption() procedure to decrypt the cover image into confidential data.

Module 2: TPA Module- A Trusted Party Authority (TPA) is responsible for identifying cloud servers and user authentication.

- Verifies authenticity of end users to access a particular cloud server
- It generates a token based on user request and system parameters
- Distributes tokens (i.e., private keys) to user and cloud server.
- The cloud server matches both the keys during data request from individual users.

Module 3: CSP Module- The cloud service provider (CSP) stores its encrypted, confidential data in the cloud server.

- The CSP module runs data_encryption() procedure to encrypt confidential data.
- Stores encrypted cover image with confidential data on cloud servers.
- Securely delivers the key to end user.

Module 4: FH_Values Module (Fibonacci series and Hash value generating Module)

The FH_Value Module generates a series of Fibonacci numbers and hash values.

- Generate Fibonacci series using Fib_series() procedure.
  - The main property of Fibonacci series is that, every 3rd number of series contains even number, however the first Fibonacci number zero is not considered. The property of fibonnaci shows every third number is even number.So targeting every third position of this series with some even number may be a highly predictable for the intruder. The third factor in this series is purposefully masked by 1.

$$F_i = 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots\ldots F_n$$

(i.e Fibonacci series without zero)

$$F_{i3} = F_{i3} + 1$$

(Where this is masking of the Fibonacci series)

$$F_i = 1, 1, 3, 3, 5, 9, 13, 21, 35, 55, 69, 145 \ldots . \mathrm{F}_n$$

(i.e Odd Fibonacci series Eliminating every 3rd position even number)

- Generate a hash value using odd Fibonacci series

$$h(F_i) = (7 + F_i^2) \bmod 251$$
$$(Where, i = 1,1,3,3,5,9,13,21,35 \ldots . F_n)$$

Module 5: Data_Encryption Module- Confidential data is encrypted using the image stenography technique by CSP (cloud service provider), by the below mentioned methodology:

- Randomly choose an image from an image repository of CSP and consider it as a cover image.
- Convert the cover image into its gray scale value matrix.
- Retrieve confidential data from database and convert it into ASCII codes.
- Call FH_Values module to will retrieve hashed values and then multiply ASCII code with hash value. Finally, obtain some number which contains confidential data.
- Randomly choose gray scale value pixels in cover image and replace it with multiplicity confidential data value.
- Using these random locations, generate a confidential key with the multiplication of Random location and hash value. This key is sent to user for decryption as a private key.
- Convert gray scale matrix into an image and store this image in the cloud server.

The confidential key can be used to decrypt the encrypted cover image.

- First, convert the cover image into its gray scale value matrix.
- Use key for finding confidential data location in this grayscale matrix.
- Call the procedure FH_Value( ) from to get hash values.
- Divide confidential data location gray scale value of hash value to get ASCII value. Hence finally confidential data or ASCII value is converted into characters.

3. Example of Plaintext to Cipher Text

In this encryption technique a sample text is taken, Example Plain text: PID Ravi

$$\text{ASCII Code: } (a_i) = 80, 73, 68, 32, 82, 97, 118, 105$$

A. Fibonacci series: $0, 1, 1, 2, 3, 5, 9, 13$
(Eliminate first number, i.e. 0 and keep 80 as it is in ASCII Code)

$$\text{Odd Fibonacci series: } (F_i): \ 1, 1, 3, 3, 5, 9, 13$$

B. Hash function: (Apply hash function which takes odd Fibonacci series as input)

$$h(F_i) = (7 + F_i^2) \bmod 251$$

i.e 8, 8,16,32,88,176
Multiply ASCII codes and hash values

$$result_i = a_i \, X \, h(f_i)$$

C. Ciphertext:
80, 584,544,512,1312,3104,1038,18480
The series Fibonacci mapped into some value Z using a hash function as a key term. It can be reprinted using mathematical form as shown below,

$$h_i : \ \mathrm{F}_i \rightarrow Z_i$$

Now this cipher text is embedded in the cover image with randomly chosen pattern.

4. System Architecture

The architecture of the system consists of four major components: User, TPA, CSP and Cloud Server. Individual users collect their data from cloud server , decrypt it and then store in their mobile devices.

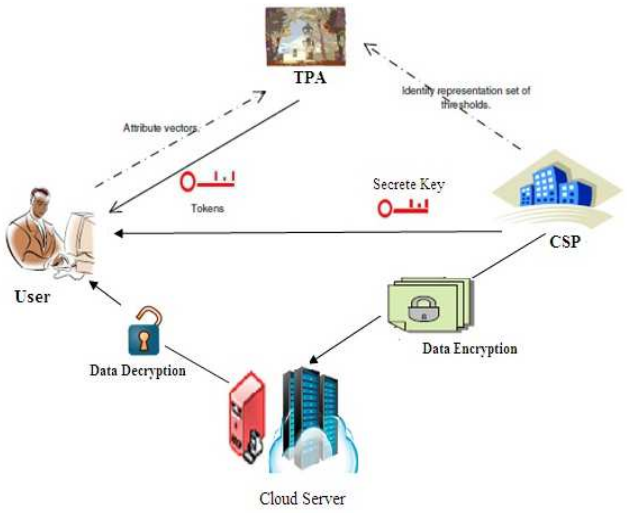

Fig. 2. *System Architecture*

The user module sends a request to TPA with their attributes like user name, password, MID, IP address and time stamp for granting the token. TPA validates username and password and prepares a token based on the request and sends it back to the end user. Decryption is done at the user side, so the secret key, necessary for decryption is sent from CSP to the user. A Trusted Party Authority (TPA) is responsible for identifying cloud servers and user authentication. The cloud service provider (CSP) stores its encrypted data in the cloud server. The cloud server stores all kinds of encrypted data and provides a rich set of resources to the end user. There are two secret key exchanges in the system: one for authentication and another one is used as private key to decrypt confidential data.

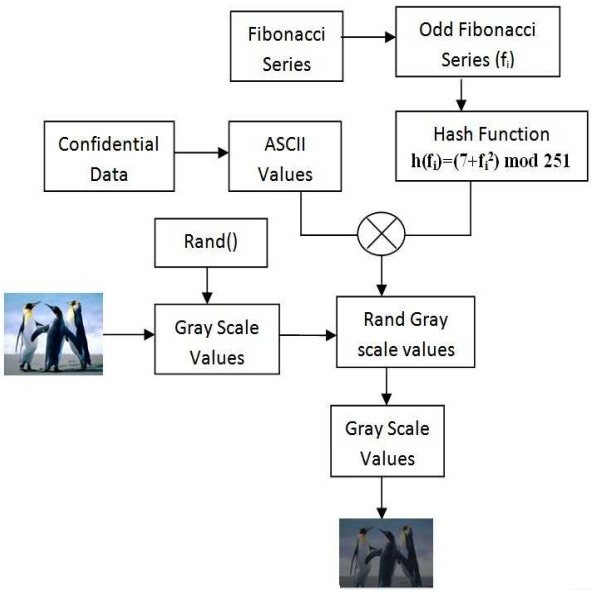

Fig. 3. *Proposed Data Encryption Technique*

Confidential data is encrypted using the image steganography technique by CSP (cloud service provider). This can be described as - Randomly choose an image from an image repository of CSP and consider it as a cover image. Next step converts the cover image into its gray scale value matrix. The confidential data are retrieved from database and convert it into ASCII codes. Next, FH_Values module is called and the hashed values are multiplied with ASCII code. Fat this point some converted number is generated which holds confidential data. Again a randomly chosen gray scale value pixel exists in the chosen image is then replaced by this newly generated confidential data value. Using these random locations, a confidential key is generated by the multiplication of random location and hash value. This key is sent to user for decryption as a private key. Thereafter, convert gray scale matrix into an image and stores this image in the cloud server.

The decryption process is carried out at the user side by calling the procedure Data_Decrypt (). At first the tentative file is downloaded from the cloud server and store it in local system. The confidential key generated for data decryption uses certain steps. First, the cover image converts

into its gray scale value matrix. A special key is used for finding confidential data location in this grayscale matrix. Once the location is identified the FH_Value () is called to obtain the hash values. The confidential data location divides the gray scale value of hash value to get ASCII value. Hence finally, confidential data or ASCII value is converted into characters.

Encryption algorithm contains two parts: static and dynamic. Fig. 3 shows the multiplication of hash value with ASCII codes is static one and whereas, choosing random pixels from cover image is the dynamic part. So our proposed method becomes a dynamic encryption algorithm, as it will increase the security level of the algorithm against cryptanalysis.

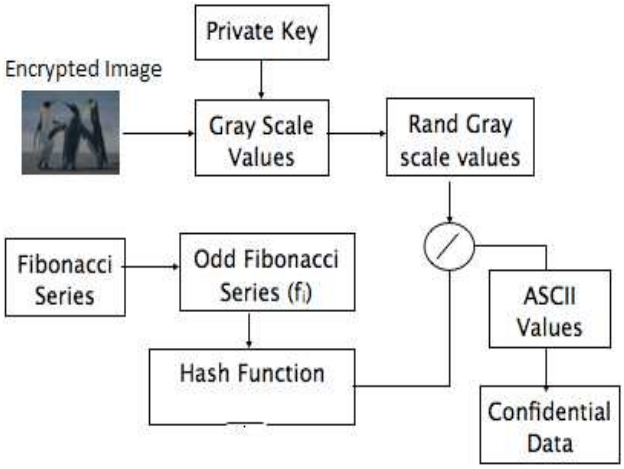

Fig. 4. *Proposed Data Decryption Technique*

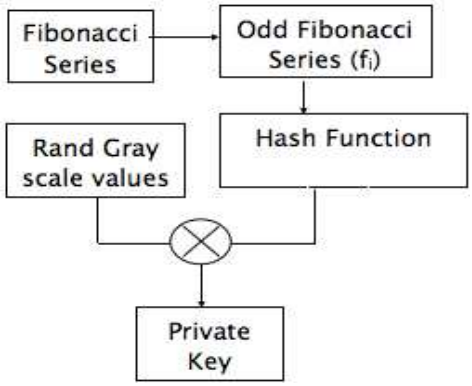

Fig. 5. *Private Key generation block diagram*

The cloud service provider will generate a private key during the encryption process. In encryption algorithm uses a random function to choose random pixel values or gray scale values to embed the confidential data as shown in block diagram fig. 2. Simultaneously cloud service provider generates a private key based on same hash function which is dynamic in nature at every time. Here random pixel value location is going to multiply by hash value to get private key as the length of the key is dependent on a number of random locations and in turn, the number of random locations is dependent on the number of characters present in confidential data. Therefore, length of the key is dependent on the number of characters going to hide into image.

The possible random values or range of random number generation is in between 0 to 256 i.e. size of the cover image and the probability of guessing these random pixel locations are 1/256.

5. Cloud User Authentication

The third component is a user or client for CSP who will have valid PID, Password and mobile ID (MID), who will be able to enter their details and get access to the confidential data stored in the cloud server. Cloud user authentication is fairly easy to achieve, because of the static nature of user validation and existing cloud authentication consist cloud id and password only. This paper addresses the issue, so that is can upgrade authentication into dynamic validation. TPA will send an id to end user mobile device (or E-mail) called MID for every user login session. MID generation is based on the TPA server system environment, which is redundant in nature. The cloud server verifies username, password and MID of a particular user login with respect to system parameter.

6. System Efficiency Factor

To solve the problem, hash function is used.

Theorem: Any set where $\{(A+B)\ MOD\ X\}$ is a finite field while $A, B \geq 0, and..X > 0$

Proof:

To prove the above mentioned statement, we need to show that the set is a non trivial Ring with unity; if it is commutative and each non-zero element is a unit. The set definition is as follows:

$$\{(A+B)\ MOD\ X\} \rightarrow \{a_0, a_1, a_2, ...a_n\}$$

Now, if A and B both are zero, then the set contains 0 as an element. Hence there is at least one element $\{0\}$ in the set. So this is non-trivial.

Since, R is a finite ring containing elements $\{a_0, a_1, a_2.....a_n\}$ of which a_0 is the zero element, then $\{a_0.a_1, a_1.a_1, a_2.a_1, ...a_n.a_1\}$ all belongs to R and $a_0.a_1 = 0$. Since R contains no divisor of zero, then all are distinct.

$$a_0.a_i = a_1.a_j$$
$$\equiv a_1(a_i - a_j) = 0$$
$$\text{since}, a_1 \neq 0$$
$$then, a_i = a_j$$

So, the $\{(A+B)MODX\}$ as a distinct non-zero elements, $\{a_0.a_1, a_1.a_1, a_2.a_1, ...a_n.a_1\}$ the continuation will come as a_1 in some cases.

Say, $a_k.a_1 = a_1$

If α is an arbitrary non-zero element in, then α can be $\{a_0.a_1, a_1.a_1, a_2.a_1, ...a_n.a_1\}$ any of these elements, then

$\alpha.a_k = \alpha; a_k.\alpha = \alpha$ for all non-zero α in R

Also $0.a_k = a_k.0 = 0$

Hence, $\alpha.a_k = \alpha$ for all α in R.

So, a_k is the unity in R.

To argue with the commutative nature of the set R. It can be said that $\{(A+B)MODX\}$ contains the elements $\{a_0, a_1, a_2.....a_n\}$ while $x > 0$. Interchanging position of A with B would not change the number of elements in the set. Again all the elements $\{a_0, a_1, a_2.....a_n\}$, are in finite order, where the heighest value can be (X-1) and the lowest is 0. Both of these are finite and belongs to set in R.

The Fibonacci series is going to generate in encryption and/or decryption module, where every third value of this series is changed by applying masking function. This issue will increase the efficiency of encryption factor. Conversion of confidential data into its equivalent ASCII character and multiply with hash values is also a strong Angus process of the newly proposed encryption algorithm. To identify a new hash function has been taken the help of the proven theorem mentioned above, where A is replaced by integer value 7, B is replaced by f_i^2 and X is replaced by 251. To generate hash value a hash function is used $h(F_i) = (7 + F_i^2) \bmod 251$. The justification of choosing the function is as described below:

Justification of Hash Function

The "251" characteristics

The Hash function used as 251 possesses many arithmetic and numerical features against cryptanalysis.

- The number which is used for hash function as a congruent number follows some special types of primes those are 251 is a regular prime, an Eisenstein prime, a Chen prime, a Gaussian prime, and Sophie Germain prime.
- 251 is also sum of three consecutive primes (79 + 83 + 89) and sum of seven consecutive primes (23 + 29 + 31 + 37 + 41 + 43 + 47).
- It must trace as odd factor 3 and 9 numbers sum.
- 251 is also the smallest number that can be written as the sum of three cubes in two ways: $251 = 1^3 + 5^3 + 5^3 = 2^3 + 3^3 + 6^3$
- Any cube is congruent to 0, 1, or −1 modulo 9. It follows that the sum of three cubes cannot be congruent to 4 or 5 modulo 9.
- There exists congruential restriction analogous to the case of two squares. By Dirichlet's Theorem, on primes in arithmetic progressions (or undoubtedly by much more elementary means) one can show that there are infinitely many primes congruent to 4 modulo 9, and also infinitely many primes congruent to 5. Thus there are infinitely many primes that cannot be represented as the sum of three cubes.
- It is important note that cover image is used for encryption algorithm having size 256 X 256, so that maximum number random pixels can choose using random value generation function ranges from 0 to 256. Nearest prime number with respect to 256 is 251 and 257 so that 251 can be chosen in hash function as a congressional factor. If modular congruent exceeds 256, then the resultant value of hash function becomes 1, 2, 3……. Which is a better way of limiting these values, thereby justifying the selection of number 251.

Why group theory?

According to number theory hash function under addition modulo 251 becomes a group (G, +). So it is important to show that the hash function used here for encryption is a finite group. Here we have to show that the elements under this group are finite in number and all the elements in the group satisfies the fundamental property of group theorem. It should satisfy following axioms with respect to the group:

1) Closure

If a and b are in present in the group then $a + b$ also presents in the group.

Hash function: (Apply hash function which takes odd Fibonacci series as input)

$$h(F_i) = (7 + F_i^2) \bmod 251$$

2) Associative

If $a, b \& c$ are present in the group then $(a + b) + c = a + (b + c)$ also present in the group.

8+8+16=48

3) Identity

There is an element e of the group such that for any element a of the group.

$$a + e = e + a = a$$

This satisfies for all the element for the given set of elements.

4) Inverse

For any element a of the group there is an element a^{-1}

$$a + a^{-1} = a^{-1} + a = e$$

This property also satisfies for all the elements in the given set of elements.

Number 7 is used in the hash function, as it is basically a prime number and exactly a regular prime or odd prime.

In encryption and decryption algorithm a mapping is going to take place in Fibonacci series fits into some value Z using a hash function as a key term. It can be reprinted using mathematical form as shown below,

$$h_i : \mathrm{F}_i \rightarrow Z_i$$

Now this is going to embed with the cipher text in the cover image with randomly chosen way. From all these

properties of the hash function is can be said that hash function makes encryption and decryption algorithm more reliable.

8. Conclusion

This work is to address an important problem and design Public Cloud User Authentication and Data Confidentiality Using Image steganography with a Hash Function system to protect the privacy of the involved parties and their data. According to information security, authentication and confidentiality need to be provided of data in a public cloud environment by lowering resource cost. A cloud service provider uses a business model called pay-as-you go for all its computations and resource supports so that data storage cost can be reduced over the computation cost of cloud.

The proposed encryption algorithm is highly secure and reliable one, which is on the basis of image steganography uses same hash value and Fibonacci series as 3 to 4 steps of twisting data to increase security level. Our security and performance analysis demonstrates the effectiveness of the proposed design.

Finally, to enable the resource constraint for small companies to participate in business data; our system design helps to shift the confidential data burden to the cloud by applying newly developed encryption technique. Our system has been shown to achieve the design objective.

Snapshots

Data Encryption Output

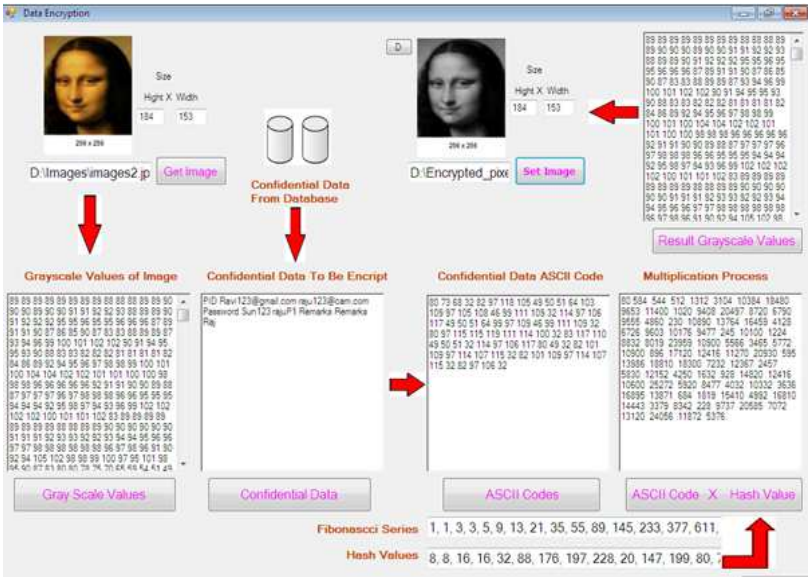

Fig. 6. *Data encryption snapshot*

Data Decryption Output

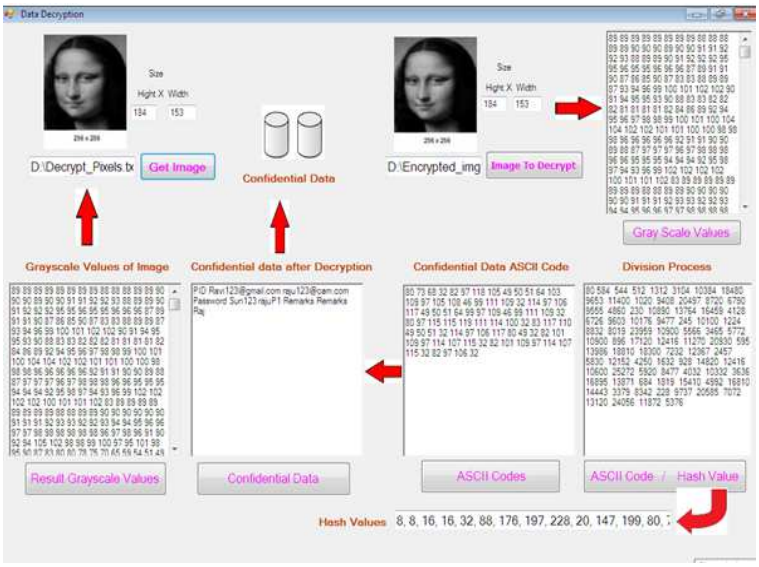

Fig. 7. *Data decryption snapshot*

References

[1] P. Mohan, D. Marin, S. Sultan, and A. Deen, "Medinet: personalizing the self-care process for patients with diabetes and cardiovascular disease using mobile telephony." Conference Proceedings of the International Conference of IEEE Engineering in Medicine and Biology Society, vol. 2008, no. 3, pp. 755–758. [Online]. Available: http://www.ncbi.nlm.nih.gov/pubmed/19162765

[2] CryptographyandNetworkSecurity; Principles and Practices (5thEdition), William Stallings,

[3] Rivest, R.; A. Shamir; L. Adleman (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". Communications of the ACM

[4] Biham, Eliand Shamir, Adi(1991). "Differential Cryptanalysis of DES-like Cryptosystems". Journal of Cryptology Bruce Schneie, Applied Cryptography, 2nd edition, Wiley, 1996

[5] A. Tsanas, M. Little, P. McSharry, and L. Ramig, "Accurate telemonitoring of parkinson's disease progression by noninvasive speech tests," Biomedical Engineering, IEEE Transactions on, vol. 57, no. 4, pp. 884– 893, 2010.

[6] G. Clifford and D. Clifton, "Wireless technology in disease management and medicine," Annual Review of Medicine, vol. 63, pp. 479–492, 2012.

[7] L. Ponemon Institute, "Americans' opinions on healthcare privacy, available: http://tinyurl.com/4atsdlj," 2010.

[8] A. V. Dhukaram, C. Baber, L. Elloumi, B.-J. van Beijnum, and P. D. Stefanis, "End-user perception towards pervasive cardiac healthcare services: Benefits, acceptance, adoption, risks, security, privacy and trust," in PervasiveHealth, 2011, pp. 478–484.

[9] M. Delgado, "The evolution of health care it: Are current u.s. privacy policies ready for the clouds?" in SERVICES, 2011, pp. 371–378.

[10] N. Singer, "When 2+ 2 equals a privacy question," New York Times, 2009.

[11] I. Neamatullah, M. Douglass, L. Lehman, A. Reisner, M. Villarroel, W. Long, P. Szolovits, G. Moody, R. Mark, and G. Clifford, "Automated de-identification of free-text medical records," BMC medical informatics and decision making, vol. 8, no. 1, p. 32, 2008.

[12] S. Al-Fedaghi and A. Al-Azmi, "Experimentation with personal identifiable information," Intelligent Information Management, vol. 4, no. 4, pp. 123–133, 2012.

[13] J. Domingo-Ferrer, "A three-dimensional conceptual framework for database privacy," Secure Data Management, pp. 193 202, 2007.

[14] AndrewSTenenbaum,"ComputerCommunicationNetworks" McGrawHill, Revised 4thedition, 2006

[15] David Kahn,"The Codebreakers-The Story ofSecretWriting",1967

[16] A. Farmer, O. Gibson, P. Hayton, K. Bryden, C. Dudley, A. Neil, and L. Tarassenko, "A real- time, mobile phone-based telemedicine system to support young adults with type 1 diabetes," Informatics in primary care, vol. 13, no. 3, pp. 171–178, 2005.

[17] M. Barni, P. Failla, V. Kolesnikov, R. Lazzeretti, A. Sadeghi, and T. Schneider, "Secure evaluation of private linear branching programs with medical applications," Computer Security–ESORICS 2009, pp. 424–439, 2009.

[18] A. C.-C. Yao, "How to generate and exchange secrets (extended abstract)," in FOCS. IEEE, 1986, pp. 162–167.

[19] Cryptography and Network Security; Principles and Practices (5th Edition), William Stallings,

[20] Rivest, R.; A. Shamir; L. Adleman (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". Communications of the ACM

[21] Biham, Eli and Shamir, Adi (1991). "Differential Cryptanalysis of DES-like Cryptosystems". Journal of Cryptology