Nikhil Gupta, et. al. International Journal of Engineering Research and Applications
www.ijera.com
ISSN: 2248-9622, Vol. 10, Issue 6, (Series-II) June 2020, pp. 31-37

RESEARCH ARTICLE OPEN ACCESS

Prevention of E-Fraud by Self-Authenticating the e-Documents

Nikhil Gupta[1] ,Kaneez Zainab[2], Sanskar Srivastava[3], Akash Agnihotri[4], Kaushal[5], Ahmed Safwan Ansari[6]
[,1,2,3,4,5,6]*Computer Science Department,*
Babu Banarasi Das National Institute of Technology and Management,Lucknow

ABSTRACT*:*
We consider a method for preventing e-Fraud in which a image is encrypted with a floating point cipher using a convolution operation and then output will generate in a image ciphertext. The output is then 'embedded' in a host image to hide the encrypted information. Decryption is accomplished by: (i) extracting the binary image from the host image; (ii) correlating the result with the original cipher. In principle, any cipher generator can be used for this purpose and the method has been designed to operate with images. The approach has a variety of applications and in this paper, we focus on the authentication and self-authentication of e-documents (letters and certificates, for example) that are communicated over the Internet and are thereby vulnerable to e-Fraud (e.g. modification, editing, counterfeiting etc.).
Keyword: e-Fraud, cipher, embedded, encrypted, decryption, authentication

---

Date of Submission: 18-05-2020 Date of Acceptance: 03-06-2020

I. INTRODUCTION

The problem of all present encryption systems is that the form of the output data (the cipher text), if interpreted, aprises the voilater to the fact that the information being shared is important and that it is therefore worth striking and attempting to decrypt it. In this case, we assume that the intercept will be attacked, decrypted and the information retrieved.

The main objective of the proposed system is to secrete the encrypted message or confidential data in to an image which further act as a carrier of confidential data and to transmit to the destination securely without any unauthorized interception. So, the data encryption and decryption into an image and steganography is used to protect the data from unauthorized access, this plays a major role in the project.

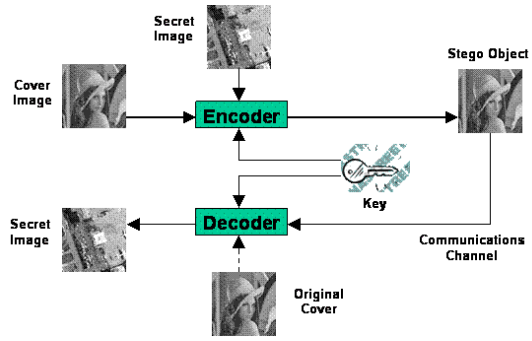

Figure 1 Flow Process

One of the reasons that unauthorized attackers can be successful is that most of the information they acquire from a system is in a form that they can read and understand. Attackers may reveal the information to others, modify it to misrepresent an individual or enterprise, or use it as a weapon to attack.

Steganography conceals the confidential message within the host data set and presence subtle and is to be securely communicated to a receiver. The host data set is purposely corrupted, but in a secret way, designed to be invisible to an information analysis.

II. PROBLEM STATEMENT

The former consists of linguistic or language forms of hidden writing. The later, such as invisible ink, try of hide messages physically. One disadvantage of linguistic steganography is that users must equip themselves to have a good knowledge of linguistry. In recent years, everything is trending toward digitization. And with the development of the internet technology, digital media can be transmitted conveniently over the network. Therefore, messages can be secretly carried by digital media by using the steganography techniques, and then be transmitted through the internet rapidly

III. SOFTWARE REQUIREMENT SPECIFICATION

This part depicts about the prerequisites. It determines the equipment and programming prerequisite that are needed for software to keeping in mind the end goal, to run the application appropriately. The Software Requirement Specification (SRS) is clarified in point of interest, which incorporates outline of this exposition and additionally the functional and non-practical necessity of this thesis

a. General Description

The reason behind the framework prerequisites and determination record is to depict the assets and administration of those assets utilized as a part of the configuration of the Public Key Cryptosystem for information partaking in distributed storage. This framework necessity and particular will likewise give insights with respect to the utilitarian and non-useful prerequisites of the venture.

b. Users Perspective

The Characteristic of this task work is to give information adaptability security while sharing information through cloud. It gives a proficient approach to share information through cloud.

c. Non Functional Requirement

Non utilitarian necessities are the prerequisites which aren't straightforwardly having an area with the precise capacity gave by the framework. This gives the standards which will be utilized to end up the operation of a framework instead of particular practices.

This can be utilized to relate the rising structure properties, as an example , immovable quality, reaction time and store inhabitancies. Here again they need to portray objectives on the system, as an example , the capacity of the info yield devices and data representation used as a bit of structure interfaces. In all probability all non-helpful essentials are often concerning the system as whole instead of to individual structure highlights. This suggests they are every now and again essential appear differently in relation to the individual commonsense necessities. Non utilitarian necessity gets through the client needs, in sight of paying plan limitations, hierarchical approaches, and therefore the requirement for interoperability with other programming and equipment frameworks.

The going with non-valuable requirements are meriting thought.

 Security: The framework ought to permit a secured correspondence between information proprietor and beneficiary.

 Reliability: The system should be trustworthy and ought not corrupt the execution of the present structure and should not to provoke the hanging of the structure.

d. System Requirement

Hardware Requirement

- **Processor** : intel/amd
- **Keyboard** : 104 Keys
- **Floppy Drive** :1.44 MB MHz Pentium III
- **RAM** : 128 MB
- **Hard Disk** : 10 GB
- **Monitor** :14" VGA COLOR
- **Mouse** :Logitech Serial Mouse
- **Disk Space** : 1 GB

Software Requirements

- **Operating System** : Win 2000/ XP
- **Server** : Apache Tomcat
- **Technologies used** : Java, Servlets, JSP, JDBC
- **JDK** : Version 1.7
- **Database** : My SQL 5.0

e. Feasibility Study

Believability is the determination of paying little respect to whether an undertaking justifies action. The framework followed in building their strength is called acceptability Study, these kind of study if a task could and ought to be taken.

Three key thoughts included in the likelihood examination are:

- Technical Feasibility
- Economic Feasibility
- Operational Feasibility

f. Technical Feasibility

Here it is considered with determining hardware and programming, this will effective fulfil the client necessity the specialized requires of the framework should shift significantly yet may incorporate.

- The office to create yields in a specified time.
- Reaction time under particular states.
- Capacity to deal with a particular segment of exchange at a specific pace.

g. Economic Feasibility

Budgetary examination is the often used system for assessing the feasibility of a projected structure. This is more usually acknowledged as cost/favourable position examination. The method is to center the focal points and trusts are typical casing a projected structure and a difference them and charges. These points of interest surpass costs; a choice is engaged to diagram and realize the system will must be prepared if there is to have a probability of being embraced. There is a consistent attempt that upgrades in exactness at all time of the system life cycle.

h. Operational Feasibility

It is for the foremost part identified with human association and supporting angles. The focuses are considered:

- What alterations will be carried through the framework?
- What authoritative shapes are dispersed?
- What new aptitudes will be needed?
- Do the current framework employee's individuals have these aptitudes?
- If not, would they be able to be prepared over the span of time?

i. Resource Requirement

Java

Java is a stage autonomous programming dialect. It is outline to be basic and convenient crosswise over diverse stages.

The java programming vernacular is an unusual state tongue that can be portrayed by most of the going with in vogue expressions:

- Object oriented
- Simple
- Architecture neutral
- Portable
- Robust
- Dynamic
- Secure

The Java API is a broad social affair of moment programming fragments that give various profitable limits, for instance, graphical customer interface (GUI) contraptions. The Java API is accumulated into collections of correlated classes and interfaces; these collections are recognized as packs.

Java stage gives you the accompanying elements:

- **The essentials:** Items, strings, strings, numbers, info, yield, information structures, framework properties, date, time et cetera.
- **Applets:** The arrangement of traditions utilized by applets.
- **Networking:** URLs, TCP, UDP attachments, and IP addresses.
- **Internationalization:** Help for composing projects that could be restricted for clients around the world. Projects can naturally adjust to particular local people and be shown in the suitable dialect.
- **Security:** Mutually low level and abnormal state, together with electronic marks, open and private key administration, right of entry control and authentications.
- **Software components:** Recognized as JavaBeans, could connect to existing parts structural designs.
- **Object Serialization:** Let's Permits lightweight tirelessness and correspondence by means of Remote Method Invocation (RMI).
- **Java Database Connectivity (JDBC):** Give consistent entree to an extensive variety of social databases.

Advantage of java technology:

- **Get started quickly:** In spite of the fact that the java programming dialect is an intense article arranged dialect, it is anything but difficult to learn, particularly for software engineers effectively acquainted using C or C++.
- **Write less code:** Examinations of undertaking estimationsadvise that a framework built in the java language tongue shall be 4 times more diminutive compare tosimilar program in C++.
- **Write better code:** Java dialect energizes great coding rehearsals and its trash gathering serves to evade memory spills. Its item introduction, its javaBeans segment building design and its far reaching, effectively extendible API let's to use again other individuals tried code and present less bugs.
- **Develop programs more quickly:** Headway time can be as much as twice as speedy against making the similar program in C++.
- **Write once, run anywhere:**Since 100% immaculate java projects are ordered into system autonomous byte codes, run reliably on whichever java stage.
- **Distribute software more easily:** Update applets smoothly from a middle server. The applets misuse the segment of allocating new classes could be stacked "on the fly", without recompiling the whole system.

Java Server Page

Java Server Pages development allows you to put scraps of servlet coding particularly into a substance based record. A java server page is a substance based record that holds two sorts of substance: static format data, which should be imparted in several substance based association, for instance, XML, WML, HTML and Java server page

segments, which choose how the page fabricates component content.

Java Server Page (JSP): An extensible Web innovation that make use of layout information, custom components, scripting dialects, and server side Java programming language articles to homecoming element substance to a customer. As indicated by JSP model1 we can build up the application as:

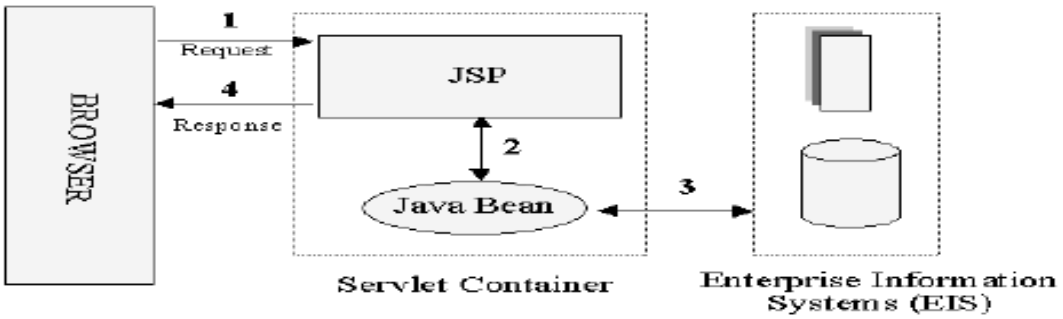

Figure 2. Architecture of jsp model 1

Commonly the layout information is XML/HTML components, and as a rule the customer is a Web programs. According to above replica the presentation method of reasoning must be executed in java server page and the business justification must be realized as a component of Javabean and this model assist us in disconnecting the appearance and business basis.

For sweeping extent reaches out instead of using model1 it is perfect to use model2 Model View Controller. Struts structure is in light of model 2.JSP allows you to specific the dynamic bit of your pages with the static HTML. Here it just makes the steady HTML in the run of the mill way, using any Web page building mechanical assemblies it frequently uses. Here again encase the dynamic code for the parts in exceptional labels, the greater part of which begin with "<%" and end with "%>". You ordinarily give your record a .jsp augmentation, and regularly introduce it in wherever you could put a typical Web page.

Despite the fact that what you compose frequently seems more like a customary HTML record compare to a servlet, in the background, the java server page just acquires change over to an average servlet, through the static HTML basically being printed to the yield stream joined with the servlet's organization method.

JavaScript

Java Script is a one of the object oriented; lightweight, script based computer programming language dialect tongue which was made by Netscape Communication Corporation. JavaScript holds the change equally client and server parts of application of Web program and the client side; this could be employ to form programs which are implemented by a Web program inside the association of a Web page on the server side, this should be employed to make a Web server programs which could deal with information set up together by a Web project and thereafter overhaul the program's showcase moreover.

Despite the fact that JavaScript underpins client and server Web programming, this lean toward JavaScript at customer side programming subsequent to a large portion of the programs bolsters this one. JavaScript is as simple as to study as HTML, and JavaScript explanations could be incorporated in HTML reports by encasing the announcements among a couple of scripting labels.

Here there are a couple of issues we can do with JavaScript

- Approve the substance of a structure and build computations.
- Include looking over or changing information to the Browser's status line.
- Invigorate pictures or pivot pictures that change when we shift the mouse above them.
- Identify the program being used and presentation distinctive substance for diverse programs.
- Identify introduced modules and inform the client if a module is needed.
- JavaScript can do a great deal more with JavaScript, including making whole application.

JavaScript and Java are altogether diverse dialects. A couple of the obvious contrasts are:

- Java applets are usually indicated for a situation inside the web chronicle; JavaScript could impact every bit of the Web report itself.
- JavaScript is most suitable to essential applications and inserting instinctive components to

Web pages and Java could be used for amazingly multifaceted applications.
Here there are various distinctive complexities yet the fundamental object to review is that JavaScript and Java are autonomous lingos. They are together useful for unmistakable objects; really they could be used both to join their ideal circumstances.

JDBC

JDBC with a last goal to set a self-administering database benchmark API for java made database blend, or JDBC. This offers a non specific SQL database access portion that provides an expected interface to a mixed pack of RDBMS. This trustworthy interface is refined in the use of "unit" database framework units, or drivers. On the off chance that a database merchant wishes to have JDBC strengthen, he or she can allot to the driver to every stage that the database and java keep running on. To get a more expansive attestation of JDBC, sun builds up JDBC's system concerning ODBC. Java database integration gives uniform access to an extensive variety of social databases. MS Access databases are utilized for rapidly overhauling the store table.
Plan objectives for JDBC are as per the following:

- **SQL Level API**

The organizers experience that their essential objective was to portray a SQL interface for java. Yet not the most diminished database interface level achievable, this is an adequately low level for strange state devices and APIs to be made. Then again, it is at an adequately abnormal state for application programming architect to use it surely. Finishing this target looks into future mechanical assembly shippers to "make" JDBC code and to cover countless difficulties from the end customer.

- **SQL Conformance**

SQL sentence structure changes as this movement from database shipper to database vender. With an end target to support a wide grouping of traders; JDBC will authorize every investigation articulation to be moved out through this to the basic database driver. This authorizes the integration unit to grip non-standard usefulness in approach that is appropriate for their clients.

- **JDBC must be implemented on top of basic database interfaces**

The JDBC SQL API must "sit" on top of other fundamental SQL level APIs. This target grants JDBC to use active ODBC level drivers by the usage of an item interface. This interface could be making an elucidation of JDBC calls to ODBC and the other route around.

- **Give a java interface that is steady with whatever is left of the java framework**

As of java's affirmation in the customer gathering thusly for, the makers feels that they should not to wander away from the present blueprint of the middle java structure.

- **Keep it simple**

These objective likely shows up in all products outline objective postings. JDBC is no special case. Sun considered that the configuration of JDBC ought to be extremely basic, taking into account stand out strategy for finishing an undertaking for every component. Permitting copy usefulness just server to confound the client of the API.

- **Keep the common cases simple**

Since as a general rule, the typical SQL calls utilize the software engineers are straightforward INSERT's, SELECTs, UPDATE's and DELETE's these request should be anything but difficult to perform with JDBC. Be that as it may, more intricate SQL explanations ought to likewise be conceivable.

IV. MODULE DESCRIPTION

Number of Modules

After careful analysis the system has been identified to have the following modules:

1. **File Upload And Encryption**
2. **Hiding Text**
3. **Text Extraction**
4. **Decryption**

i. File Upload And Encryption:

Admin upload the files using filename and fileid. The user will search the uploaded files and choose file and send request to admin. Admin view the user requested file and send secret key with image during which text embed into the image .The binary image should be converted in to dam of bytes using serialization. The key will encrypt using an encryption algorithm. Use the encryption function to encrypt the numeric plaintext values using the general public key. The encrypted function gives an integer value, and then converts the integer value in to hexadecimal value. Concatenate the hexadecimal value to make a cipher text.

ii. Hiding Text:

Steganography is that the process of hiding the one information in to other sources of data like text, image or audio file in order that it's not visible to the natural view. Here, the image is encrypted, then encrypted information hidden during a host image it's an easy approach to embedding a message in to the image. The Least Significant Bit insertion

varies consistent with number of bits in a picture . The encrypted text is hiding in changed to the little bit of secret message. The encrypted information is hidden during a cover image is named as stegoimage. The stego key's wont to extract the hidden data from a stegoimage. The stego key's a secret key wont to protect the hidden message in a picture .

iii. Text Extraction:

The hidden text is extracted from the host image employing a stego key. The stego key's wont to extract the text from the image. Extract the text from an image; finally get the key data and therefore the hidden message stored during a file.

iv. Decryption:

The encrypted information extract from a picture and employing a private key to decrypt the hiddenmessage. Break the ciphertext into small blocks of knowledge that are an equivalent length because the public key modulus. The blocks of data containing a hexadecimal string. Use the decryption function to decrypt the integer values using the private key. Represent each decrypted value as a pair of bytes. By using decryption the ciphertext convert in to dam of bytes .After decryption the bytes converted in to binary image using deserialization.

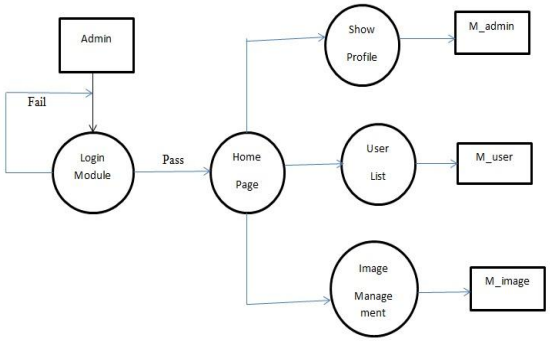

Figure 2. DFD Admin Session

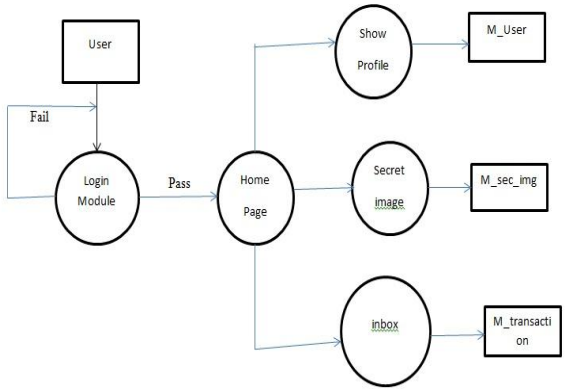

Figure 3. DFD User Session

V. RESULT

E-Fraud Prevention based on the Self-Authentication of e-Documents techniques make changes in the data to such an extent that data quality gets improved. e-Fraud Prevention based on the Self-Authentication of e-Documents techniques are used to cater to such scenarios because they are able to recover original data from watermarked data and ensure data quality to some extent. However, these techniques are not robust against malicious attacks—particularly those techniques that target some selected tuples for watermarking. In this paper, a novel e-Fraud Prevention based on the Self-Authentication of e-Documents is presented. The main contribution of this work is that it allows recovery of a large portion of the data even after being subjected to malicious attacks. A number of experiments have been conducted with different number of tuples attacked. The results of the experimental study show that, even if an intruder deletes, adds or alters up to 50 percent of tuples, e-Fraud Prevention based on the Self-Authentication of e-Documents is able to recover both the embedded watermark and the original data.

VI. CONCLUSION

E-Fraud Prevention based on the Self-Authentication of e-Documents is a really interesting subject and outside of the mainstream cryptography and system administration that most of us deal with day after day.

Steganography can be used for hidden communication. A stego-key has been applied to the system during embedment of the message into the cover image.

The master work of this application is in supporting any type of pictures without need to convert to bitmap, and lower limitation on file size to hide, because of using maximum memory space in pictures to hide the file.

Since ancient times, man has found a desire in the ability to communicate covertly. The recent explosion of research in watermarking to protect intellectual property is evidence that steganography is not just limited to military or espionage applications. Steganography, like cryptography, will play an increasing role in the future of secure communication in the “digital world”.

Future Scope

We can use this technique in mobile phone for images authentication and every place where we are using images. We can encrypt image using Advanced Encryption Techniques then store in another image it will provide more security.

REFERENCES

[1]. (2015, Feb. 26). Securing outsourced consumer data. [Online]. Available: http://databreaches.netsecuring-outsourced-consumer-data/

[2]. (2017, Jun. 3). As patients' records go digital, theft and hacking problems grow. [Online]. Available: http://kaiserhealthnews. org/Stories/2012/June/04/ electronic-health-records-theft-hacking. aspx

[3]. P. W. Wong, "A public key watermark for image verification and authentication," in Proc. IEEE Int. Conf. Image Process., 1998, vol. 1, pp. 455–459.

[4]. F. A. Petitcolas, "Watermarking schemes evaluation," IEEE Signal Process. Mag., vol. 17, no. 5, pp. 58–64, Sep. 2000.

[5]. R. Agrawal and J. Kiernan, "Watermarking relational databases," in Proc. 28th Int. Conf. Very Large Data Bases, 2002, pp. 155–166.

[6]. S. Subramanya and B. K. Yi, "Digital rights management," IEEE Potentials, vol. 25, no. 2, pp. 31–34, Mar.-Apr. 2006.

[7]. K. Bache and M. Lichman. (2013). UCI machine learning repository [Online]. Available: http://archive.ics.uci.edu /ml

[8]. R. Hassan, B. Cohanim, O. De Weck, and G. Venter, "A comparison of particle swarm optimization and the genetic algorithm," in Proc. 46th AIAA/ASME/ASCE/AHS/ASC Struct., Struct. Dyn. Mater. Conf., 2005, pp. 1–13.

[9]. T. M. Cover, J. A. Thomas, and J. Kieffer, "Elements of information theory," SIAM Rev., vol. 36, no. 3, pp. 509–510, 1994.

[10]. M. Mitchell, An introduction to genetic algorithms. Cambridge, MA, USA: MIT Press, 1996.

[11]. K. Jawad and A. Khan, "Genetic algorithm and difference expansion based reversible watermarking for relational databases," J. Syst. Softw., vol. 86, no. 11, pp. 2742–2753, 2013.

[12]. D. M. Thodi and J. J. Rodriguez, "Prediction-error based reversible watermarking," in Proc. IEEE Int. Conf. Image Process. 2004, vol. 3, pp. 1549–1552.

[13]. M. E. Farfoura, S.-J. Horng, J.-L. Lai, R.-S. Run, R.-J. Chen, and M. K. Khan, "A blind reversible method for watermarking relational databases based on a time-stamping protocol," Expert Syst. Appl., vol. 39, no. 3, pp. 3185–3196, 2012.