World Journal of Engineering Research and Technology
WJERT
www.wjert.org
SJIF Impact Factor: 4.326

DESIGN AND IMPLEMENTATION OF A TRIPLE "A" (ACCOUNTABILITY, ACCESSIBILITY AND AUTHENTICATION) SYSTEM USING IMAGE STEGANOGRAPHY

[1]*ILO Somtoochukwu F., [2]Ofoji Chigozie, and [3]Okah Paul-Kingsley

[1,2]Computer Engineering Department, Michael Okpara University of Agriculture, Umudike.
[3]Electronic and Computer Engineering Department, Nnamdi Azikiwe University Awka.

Article Received on 24/09/2017 **Article Revised on 17/10/2017** **Article Accepted on 07/11/2017**

***Corresponding Author**
ILO Somtoochukwu F.
Computer Engineering Department, Michael Okpara University of Agriculture, Umudike.

ABSTRACT

The significance of digital information security has been heightened due to advances in internet communication. The security of server-client communication over the internet is a critical issue due to digital eavesdroppers. Generally, username and password authentication is required for establishing a connection between server and client environment. The client username and password are verified by the server ends to establish a valid connection. Successful username and password verification initiates the client and server to perform further secure request and response mechanisms. This paper proposed a secure username and password transmission over the internet for authentication of server-client environment using encryption and image steganography. Client username and password are first encrypted and embedded in an image using steganographic algorithm at client side and transmitted over unsecured network to the web server. On the other side, the server extracts the username and password from image steganography decoding algorithm, decrypt and verified it's with SQL database server. In case if the intruder steals the image over network he/she will be unable to decode the password from the image.

KEYWORDS: Cover-Image, Message, Stego-Image, Stego-Key, Encryption, Decryption.

I. INTRODUCTION

The idea of having to identify oneself before being allowed to perform certain actions is quite acceptable, and expected, in today's society. People understand that this is a required step in the process of maintaining a secure environment and generally accept it. Regardless of this understanding and acceptance, however, authenticating users in a computer environment both unobtrusively and securely remains problematic. As the number of users in a network increases considerably, more challenges arises in terms of data and information storage and transmission over the internet. Example of this information include account number and password which are vital and confidential information that needs to be secured from interception by eavesdroppers. Information security is playing a vital role in many sectors such as financial institutions, private and government organizations, hospitals and e-commerce transactions. Generally, most communications are dealt in a server-client environment; hence, providing security for server-client authentication over the internet is a critical issue due to open world digital eavesdroppers.

Generally, a client-server environment is a model of computing of a distributed application structure that partitions tasks or workloads between the providers of a resource or service, called servers, and service requesters, called clients. One of the best forms of the client-server model is the internet. In this situation, the client, known as a web browser such as internet explorer and chrome are typically used as a client to interact with websites which resides on internet servers. Most times, this interaction requires an authentication of client and server environment.

Username and password authentication is one of the simplest and the most convenient authentication mechanisms over insecure networks. It provides the legal users to use the resources of the remote systems. Many Internet applications are based on username and password authentication, for example, remote login, database management systems and cloud storage server systems. However, the current Internet environment is vulnerable to various attacks such as replay attack, guessing attack, modification attack, and stolen verifier attack. Therefore, a number of researchers have proposed several username and password authentication schemes for secure login of authorized users. Major challenge is implementing a good authentication scheme which should maintain the equilibrium between security, integrity and availability. Also provision for rich usability functionalities on an authentication scheme is a necessity in modern unsecured network contexts.

This research study proposes a novel method of secure username and password transmission over internet for authentication using cryptography with image steganography. Username and password on the client application is encrypted, embedded in an image using steganography techniqueand then transferred over an insecure network (such as the internet) to the server machine. On the other side, the server receives that image, extracts the encrypted username and password from stego-image, decrypt the message and then verifies it with its backend SQL database server.

II. LITERATURE REVIEW

This section reviews various works by different writers and researchers on image steganography in improving data and information security. There are many different proposed methods available, which used image steganography for authentication but for different purposes.

Review of Relevant Literature

Y. K. Jain and R. R. Ahirwal,(2010)proposed an adaptive least significant bit spatial domain embedding method. This method divides the image pixels' ranges (0-255) and generates a stego-key. This private stego-key has 5 different gray level ranges of image and each range indicates to substitute fixed number of bits to embed in least significant bits of image. The strength of this proposed method is its integrity of secret hidden information in stego-image and high hidden capacity. The limitation is to hide extra bits of signature with hidden message for its integrity purpose. It also proposed a method for color image just to modify the blue channel with this scheme for information hiding. This method is targeted to achieve high hidden capacity plus security of hidden message.

Yang *et al*, (2009)proposed an adaptive LSB substitution based data hiding method for image. To achieve better visual quality of stego-image, it takes care of noise sensitive area for embedding. Proposed method differentiates and takes advantage of normal texture and edges area for embedding. This method analyzes the edges, brightness and texture masking of the cover image to calculate the number of k-bit LSB for secret data embedding. The value of k is high at non-sensitive image region and over sensitive image area, k value remains small to balance overall visual quality of image. The LSB's (k) for embedding is computed by the high-order bits of the image. It also utilizes the pixel adjustment method for better stego-image visual quality through LSB substitution method. The overall result shows a good high hidden capacity, but dataset for experimental results are limited.

S. Channalli and A. Jadhav, (2009)proposed LSB based image hiding method. Common pattern bits (stego-key) are used to hide data. The LSBs of the pixel are modified depending on the (stego-key) pattern bits and the secret message bits. Pattern bits are combination of M*N size rows and columns (of a block) and with random key value. In embedding procedure, each pattern bit is matched with message bit, if satisfied it modifies the 2nd LSB bits of cover image otherwise remains the same. This technique targets to achieve security of hidden message in stego-image using a common pattern key. This proposed method has low hidden capacity because single secret bit requires a block of (M*N) pixels.

C. H. Yang et al, (2008)proposed a Pixel value difference (PVD) and simple least significant bit's schemes are used to achieve adaptive least significant bit's data embedding. In pixel value differencing (PVD) where the size of the hidden data bits can be estimated by difference between the two consecutive pixels in cover image using simple relationship between two pixels. PVD method generally provides a good imperceptibility by calculating the difference of two consecutive pixels which determine the depth of the embedded bits. Proposed method hides large and adaptive k-LSB substitution at edge area of image and PVD for smooth region of image. So in this way the technique provides both larger capacity and high visual quality according to experimental results. This method is complex due to adaptive k generation for substitution of LSB.

K. H. Jung et al, (2008)proposed a method of Multi-Pixel Differencing (MPD) which used more than two pixels to estimate smoothness of each pixel for data embedding and it calculate sum of difference value of four pixels' block. For small difference value, it uses the LSB otherwise for high difference value, it uses MPD method for data embedding. Strength is its simplicity of algorithm but experimental dataset is too limited.

H. Zhang et al, (2009)proposed another pixel value differencing method, it used the three pixels for data embedding near the target pixel. It uses simple k-bit LSB method for secret data embedding where number of k-bit is estimated by near three pixels with high difference value. To retain better visual quality and high capacity it simply uses optimal pixel adjustment method on target pixels. Advantage of method is histogram of stego-image and cover-image is almost same, but dataset for experiments are too small.

W. J. Chen et al, (2010)introduced a high capacity of hidden data utilizing the LSB and hybrid edge detection scheme. For edge computation, two types of canny and fuzzy edges detection method applied and simple LSB substitution is used to embed the hidden data. This scheme is successful to embed data with higher peak signal to noise ratio (PSNR) with normal LSB based embedding. The proposed scheme is tested on limited images dataset.

Madhu *et al*, (2010) proposed an image steganography method, based on LSB substitution and selection of random pixel of required image area. This method is target to improve the security where password is added by LSB of pixels. It generates the random numbers and selects the region of interest where secret message has to be hidden. The strength of method is its security of hidden message in stego-image, but has not considers any type of perceptual transparency.

H. Motameni et al, (2007)introduced a data hiding technique where it finds out the dark area of the image to hide the data using LSB. It converts it to binary image and labels each object using 8 pixels' connectivity schemes for hiding data bits. This method required high computation to find dark region its connectivity and has not tested on high texture type of image. Its hiding capacity totally depends on texture of image.

Theoretical Framework

Steganography is the art of hiding and transmitting data through apparently innocuous carriers to conceal the existence of data. Steganography means to conceal messages existence in another medium. Most steganography systems use multimedia objects like image, audio, video etc. as cover media because people often transmit digital images over email or share them through other internet communication application. Steganography techniques does not alter the structure of the secret message, but hides it inside a cover-object (carrier object). After hiding process, cover object and stego-object (carrying hidden information object) are similar. So, steganography (***hiding information***) and cryptography (***protecting information***) are totally different from one another. Due to invisibility or hidden factor it is difficult to recover information without known procedure in steganography. Detecting procedure of steganography known as ***Steganalysis***.

Based on the type of the cover object, there are many suitable steganographic techniques which are followed in order to obtain security. The various types include the following:

- **Image Steganography:** Using an image as a cover object in steganography is known as image steganography. Generally, in this technique pixel intensities are used to hide the information.

- **Network Steganography:** When taking cover object as network protocol, such as TCP, UDP, ICMP etc. where protocol is used as carrier, is known as network protocol steganography. In the OSI network layer model there exist covert channels where steganography can be achieved in unused header bits of TCP/IP fields.
- **Video Steganography:** is a technique to hide any kind of files or information into digital video format. Video (combination of pictures) is used as carrier for hidden information. Generally discrete cosine transform (DCT) alter values (*e.g.,* 8.667 to 9) which is used to hide the information in each of the images in the video, which is not noticeable by the human eye.
- **Audio Steganography:** When taking audio as a carrier for information hiding it is called audio steganography. It has become very significant medium due to voice over IP (VOIP) popularity.
- **Text Steganography:** General technique in text steganography, such as number of tabs, white spaces, capital letters, just like Morse code and *etc.* is used to achieve information hiding.

III. MATERIALS AND METHODS

Materials Used

There are several alternatives and choices in term of software development tools, platform, system and technology. In implementing the proposed system, the following materials were used:

1. Personal Computer (Development Machine).
2. Microsoft .NET Framework (Software technology).
3. C# Programming language.
4. Microsoft Visual Studio 2012 (Integrated Development Environment, IDE).

Personal Computer: This served as the development and testing machine during the project implementation. Personal computer (PC) is a multi-purpose electronic computer whose size, capabilities, and price make it feasible for individual use. PCs are intended to be operated directly by an end-user, rather than by a computer expert or technician. Computers were invented to compute and solve complex mathematical problems, but today, due to media dependency and the everyday use of computers, it is seen that computing is the least important thing computers do.

The Microsoft .NET Framework: is a technology that supports building and running the next generation of application and XML web services. The .NET Framework Class Library has thousands of valuable prebuilt classes that have been tested and tuned to maximize performance. Some features of the .NET framework include the following:

1. **Common Language Runtime, CLR:** The **(CLR)**, a key part of the .NET Framework, executes .NET programs and provides functionality to make them easier to develop and debug. The CLR is a **virtual machine** (**VM**) - software that manages the execution of programs and hides from them the underlying operating system and hardware. The source code for programs that are executed and managed by the CLR is called *managed code*. The CLR provides various services to managed code, such as integrating software components written in different .NET languages, error handling between such components, enhanced security, automatic memory management and more. Unmanaged-code programs do not have access to the CLR's services, which makes unmanaged code more difficult to write.
2. **Platform Independence:** If the .NET Framework exists and is installed for a platform, that platform can run any.NET program. The ability of a program to run without modification across multiple platforms is known as ***platform independence***. Code written once can be used on another type of computer without modification, saving time and money. In addition, software can target a wider audience. Previously, companies had to decide whether converting their programs to different platforms - a process called ***porting*** - was worth the cost. With .NET, porting programs is no longer an issue, at least once .NET itself has been made available on the platforms.
3. **Language Interoperability:** The .NET Framework offers a high level of language interoperability. Because software components written in different .NET languages (such as C# and Visual Basic) are all compiled into MSIL, the components can be combined to create a single unified program. Thus, MSIL allows the .NET Framework to be ***language independent***.

C# Programming Language: is a modern, general-purpose, object-oriented programming language developed by Microsoft and approved by European Computer Manufacturers Association **(**ECMA) and International Standards Organization (ISO). C# was developed by Anders Hejlsberg and his team during the development of .Net Framework. It is designed for Common Language Infrastructure (CLI), which consists of the executable code and runtime environment that allows use of various high-level languages on different computer platforms and architectures. C# was used as the programming language for developing the proposed system due to the following reason:

1. It produces efficient programs
2. It is object oriented
3. It is a structured language
4. It can be compiled on a variety of computer platforms
5. It is a part of .Net Framework

The Microsoft Visual Studio 2012: Microsoft Visual Studio is an integrated development environment (IDE) from Microsoft. It is used to develop computer programs for Microsoft Windows, as well as web sites, web apps, web services and mobile apps. Visual Studio uses Microsoft software development platforms such as Windows API, Windows Forms, Windows Presentation Foundation, Windows Store and Microsoft Silverlight. It can produce both native code and managed code. Visual Studio includes a code editor supporting IntelliSense (the code completion component) as well as code refactoring. The integrated debugger works both as a source-level debugger and a machine-level debugger. Other built-in tools include a code profiler, forms designer for building GUI applications, web designer, class designer, and database schema designer. It accepts plug-ins that enhance the functionality at almost every level - including adding support for source control systems and adding new toolsets like editors and visual designers for domain-specific languages or toolsets for other aspects of the software development lifecycle (like the Team Foundation Server client: Team Explorer).

Methods

Methods are set of techniques or procedures that is followed in the analysis and or design of a system. The methods of software design consist of processes to conceptualize the system requirements into system implementation. The analysis and design takes the user requirements as challenges and tries to find optimum solution. For a software system such as the one proposed by this study; while the software is being conceptualized, a plan is drawn out to find the best possible design for implementing the intended solution. Three methods were integrated in the implementation of the proposed system. These are:

- Structured design analysis,
- object oriented design approach
- bottom up method

Structured design analysis: is a conceptualization of problem into several well-organized elements of solution. It is basically concerned with the solution design. Benefit of structured design is; it gives better understanding of how the problem is being solved. Structured design also makes it simpler for designer to concentrate on the problem more accurately. Structured design is mostly based on 'divide and conquer' strategy where a problem is broken into several small problems and each small problem is individually solved until the whole problem is solved. The small pieces of problem are solved by means of solution modules. Structured design emphasizes that these modules be well organized in order to achieve precise solution.

These modules are arranged in hierarchy. They communicate with each other. A good structured design always follows some rules for communication among multiple modules, namely:

- **Cohesion:** grouping of all functionally related elements.
- **Coupling:** communication between different modules.

A good structured design has high cohesion and low coupling arrangements.

Object oriented design: This works around the entities and their characteristics instead of functions involved in the software system. This design strategy focuses on entities and its characteristics. The whole concept of software solution revolves around the engaged entities. Some important concepts of Object Oriented Design are:

- **Objects:** All entities involved in the solution design are known as objects. For example, person and company are treated as objects. Every entity has some attributes associated to it and has some methods to perform on the attributes.
- **Classes:** A class is a generalized description of an object. An object is an instance of a class. Class defines all the attributes, which an object can have and methods, which defines the functionality of the object. In the solution design, attributes are stored as variables and functionalities are defined by means of methods.
- **Encapsulation:** In object oriented design, the attributes (data variables) and methods (operation on the data) are bundled together and is called ***encapsulation***. Encapsulation not only bundles important information of an object together, but also restricts access of the data and methods from the outside world. This is called information hiding.
- **Inheritance:** Object oriented design allows similar classes to stack up in hierarchical manner where the lower or sub-classes can import, implement and re-use allowed

variables and methods from their immediate super classes. This property of object oriented design is known as inheritance. This makes it easier to define specific class and to create generalized classes from specific ones.

- **Polymorphism:** Object oriented design languages provide a mechanism where methods performing similar tasks but vary in arguments, can be assigned same name. This is called polymorphism, which allows a single interface performing tasks for different types. Depending upon how the function is invoked, respective portion of the code gets executed.

Top down design: Top-down design takes the whole software system as one entity and then decomposes it to achieve more than one sub-system or component based on some characteristics. Each sub-system or component is then treated as a system and decomposed further. This process keeps on running until the lowest level of system in the top-down hierarchy is achieved. Top-down design is more suitable when the software solution needs to be designed from scratch and specific details are unknown.

The Proposed System

Major challenge is implementing a good authentication scheme which should maintain the equilibrium between security, integrity and availability. Providing rich usability functionalities on an authentication scheme is a necessity in modern unsecured network contexts. The proposed system uses a novel method of secure username and password transmission over internet for authentication using cryptography with image steganography. Username and password on the client web browser is first encrypted and embedded in an image using steganography technique. Secondly, it is transferred over an insecure network (internet) to the server machine. On the other side, the server receives that image and extracts the encrypted username and password from stego-image and decrypt the message and verifies it with its backend SQL database server.

The block diagram of the proposed system

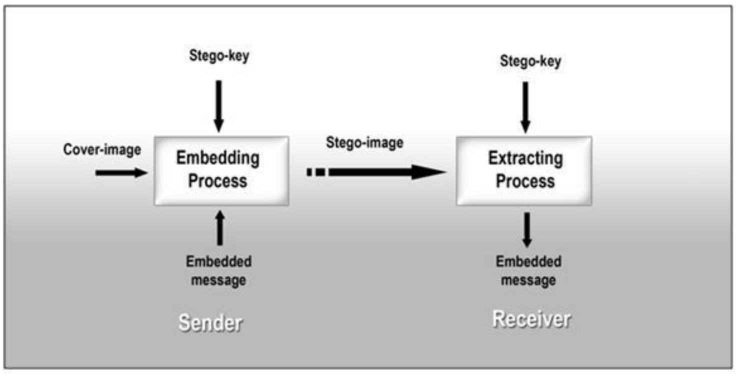


Figure 3.1: System Block Diagram

Embedding Algorithm

Real Image and data to Embed in byte array format is given as input.

1) Load the vessel image into memory.

2) Get a "readable pen" for the memory image.

3) Get width and height of the memory image.

4) Generate a threshold value.

5) Loop for all rows of memory image

Loop for all cols of memory image

a) Using the "readable pen" get red, green and blue values of current pixel.

b) if red <= threshold and green <= threshold and blue <= threshold then

* mark the pixel as NOISY (store in a list).

6) If NOISY pixel list size >= size of data to embed go to step 8.

7) Raise Error "Content length is more than embedding capacity of Vessel Image".

8) Convert the Data to embed into SECRET BLOCKS

a) Create an empty list to hold secret blocks

b) Loop for every bytes of input data

* conjugate the byte

* store the conjugated byte into secret block list.

9) Get a "writable pen" for the memory image.

10) Loop for every element of NOISY pixel list

a) Embed 2 bytes of data from SECRET blocks into red, green and blue bands of noisy pixel.

b) Using the writable pen write the pixel into memory image.

11) Write back the memory image into IMAGE FILE.

Extraction Algorithm

Image having embedded data is given as input:

1) Load the image into memory.

2) Get a "readable pen" for the memory image.

3) Get width and height of the memory image.

4) Generate a threshold value.

5) Loop for all rows of memory image

Loop for all cols of memory image

a) Using the "readable pen" get red, green and blue values of current pixel.

b) If red <= threshold and green <= threshold and blue <= threshold then

mark the pixel as NOISY (store in a list)

6) Loop for every element of NOISY pixel list

a) Extract bytes of data from red, green and blue bands of noisy pixel.

b) De-conjugate the secret blocks and form data bytes.

c) Concatenate the data in a result buffer.

7) Write back the result buffer into a FILE Input data will be image having embedded data. Load the imageinto memory. Get width and height of the memory image. Generate a threshold value.

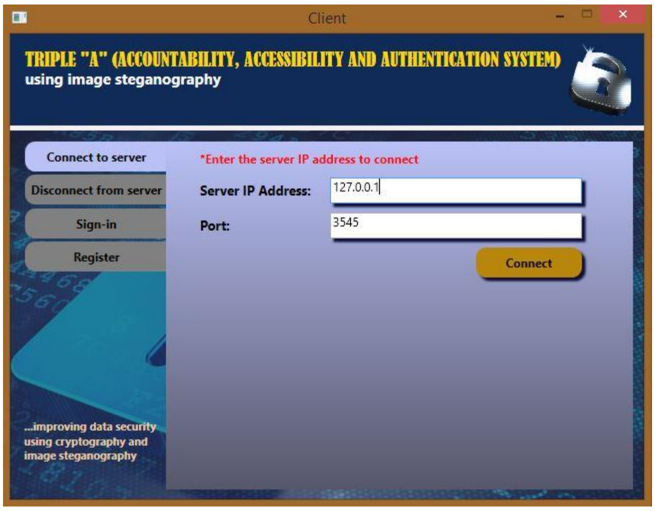
IV. SOFTWARE IMPLEMENTATION, TESTING AND ANALYSIS

Implementation

Implementation is concerned with the realization of a technical specification or algorithm as a program, software component, or other computer system through computer programming and deployment. Before the new system was effectively designed and implemented, an in-depth study of the current system was carried out in order to get a better idea that can effectively serve the system and then develop a better data security system. The objective of the software design is to improve data security in a client/server environment using cryptography and image steganography. The system was implemented using the C# programming language

RESULT

The results of the implementation are presented as screenshots of the graphical user interface (GUI) of the developed software. The system comprises of two software, the client and the server software. Like in most client-Server environment, the server is always turned on waiting for client’s connection. A client connects to the server using the server’s IP address and a port number. When the client is connected to the server, it is enabled for user registration and login. The login details needed for access authentication are encrypted, embedded into the selected image and then transmitted to the server. The stego-image is received by the server which performs an extraction and decryption process to retrieve the login details. These details are checked in the database to ensure the validity and authorization of users



Client

TRIPLE "A" (ACCOUNTABILITY, ACCESSIBILITY AND AUTHENTICATION SYSTEM)
using image steganography

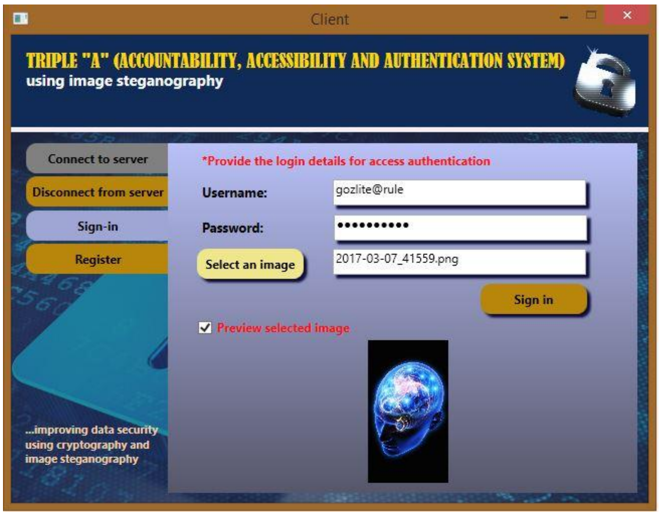
*Enter the server IP address to connect

Server IP Address: 127.0.0.1

Port: 3545

...improving data security using cryptography and image steganography

Figure 4.1: Connect-To-Server Window.



Client

TRIPLE "A" (ACCOUNTABILITY, ACCESSIBILITY AND AUTHENTICATION SYSTEM)
using image steganography

*Provide the login details for access authentication

Username: gozlite@rule

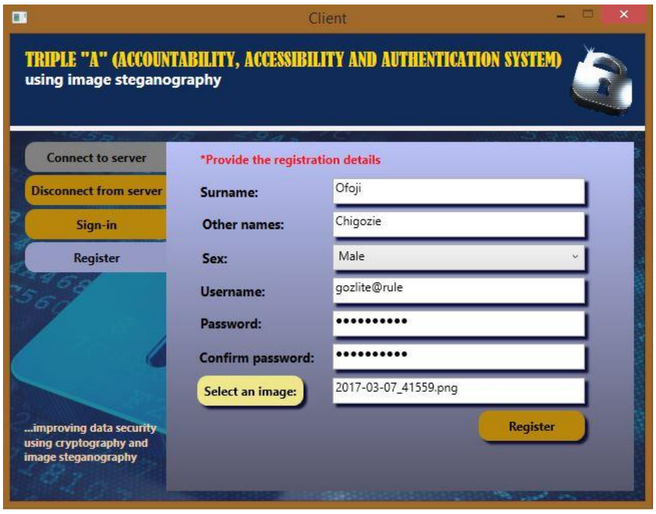
Password: ••••••••••

Select an image: 2017-03-07_41559.png

☑ Preview selected image

...improving data security using cryptography and image steganography

Figure 4.2: Sign-in Window.


Client
TRIPLE "A" (ACCOUNTABILITY, ACCESSIBILITY AND AUTHENTICATION SYSTEM)
using image steganography
Connect to server
Disconnect from server
Sign-in
Register
...improving data security using cryptography and image steganography
Select an image:
Register

*Provide the registration details

Surname: Ofoji

Other names: Chigozie

Sex: Male

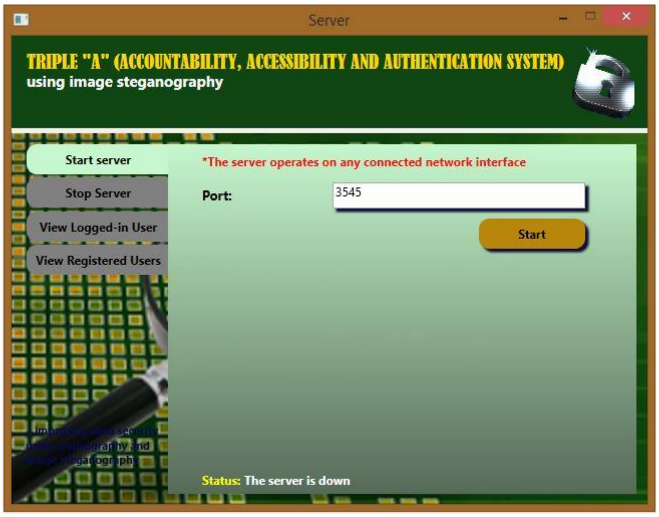
Username: gozlite@rule

Password: ••••••••••

Confirm password: ••••••••••

Select an image: 2017-03-07_41559.png

Figure 4.3: Registration Window.

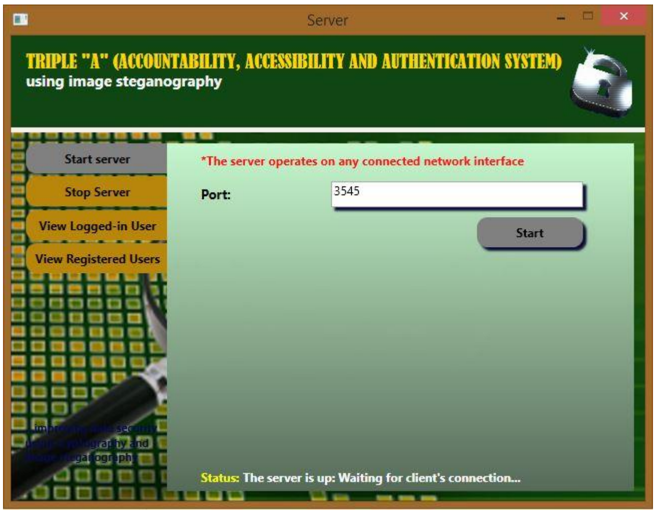

Server
TRIPLE "A" (ACCOUNTABILITY, ACCESSIBILITY AND AUTHENTICATION SYSTEM)
using image steganography
Start server
Stop Server
View Logged-in User
View Registered Users
Start

*The server operates on any connected network interface

Port: 3545

Status: The server is down

Figure 4.4: Start Server Window (Down).


Server
TRIPLE "A" (ACCOUNTABILITY, ACCESSIBILITY AND AUTHENTICATION SYSTEM)
using image steganography
Start server
Stop Server
View Logged-in User
View Registered Users
Start

*The server operates on any connected network interface

Port: 3545

Status: The server is up: Waiting for client's connection...

Figure 4.5: Start Server Window (Up).

Testing and Evaluation

This developed system was tested and evaluated in a client-server environment to ensure its proper functionality and workability. This environment consisted of two personal computers (PC) which were connected together in a local area network (LAN). It was tested in both a wired and wireless network. One of the PCs was used as a client while the acted as a server. The client system enables the registration and login of user.

V. CONCLUSION

Over the last two decades, the rapid development of internet requires confidentialinformation that needs to be protected from the unauthorized users. Most systems in a client-server environment rely solely on a valid user ID and password to prove one's identity. Since this is usually the only access requirement, it's worth putting your authentication system security practices under a magnifying glass to uncover any authentication weaknesses. Due to the security threats imposed by unsecure network, it is of utmost importance to devise and develop security measures to curtail these threats. The proposed system applies cryptography and image steganography to achieve this security measure. There are various applications in steganography; it varies among the user requirements such as copyright control, covert communication, smart ID's, printers etc. But generally, it is applied in areas where information security is highly required.

REFERENCES

1. Mehdi Hussain et al (2015), "Secure Password Transmission for Web Applications over Internet using Cryptography and Image Steganography"; International Journal of Security and Its Applications, 2015; 9(2): 179-188.
2. Anderson, R. J. (1996), "Stretching the limits of Steganography, in Information Hiding"; Springer Lecture Notes in Computer Science, 1996; 1174: 39-48.
3. Mehdi Hussain and Mureed Hussain (2013), "A Survey of Image Steganography Techniques"; International Journal of Advanced Science and Technology, May 2013; 54.
4. W. Luo, F. Huang, J. Huang (2010), "Edge adaptive image steganography based on LSB matching revisited"; IEEE Transactions on Information Forensics and Security, 2010; 5(2): 201–214.
5. Hussain, M. Hussain, M. (2010), "Pixel intensity based high capacity data embedding method"; IEEE International Conference Information and Emerging Technologies (ICIET), Pakistan, June 2010.

6. Hussain, M. and Hussain, M. (2011), "Embedding data in edge boundaries with high PSNR"; Proceedings of 7th International Conference on Emerging Technologies (ICET 2011), Sept 2011; 1-6.
7. Mehdi Hussain and Mureed Hussain (2013), "A Survey of Image Steganography Techniques"; International Journal of Advanced Science and Technology, May 2013; 54.
8. Y. K. Jain and R. R. Ahirwal (2010), "A Novel Image Steganography Method with Adaptive Number of Least Significant Bits Modification Based on Private Stego-Keys"; International Journal of Computer Science and Security (IJCSS), 2010 March 1; 4.
9. H. Yang, X. Sun and G. Sun (2009), "A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution", Journal: Radio engineering, 2009; 18(4): 509-516.
10. S. Channalli and A. Jadhav (2009), "Steganography an Art of Hiding Data"; International Journal on Computer Science and Engineering, IJCSE, 2009; 1(3).
11. C. H. Yang et al (2008), "Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems"; IEEE Transactions on Information Forensics and Security, 2008 September 3; 3: 488-497.
12. K.-H. Jung, K.-J. Ha and K.-Y. Yoo (2008), "Image data hiding method based on multi-pixel differencing and LSB substitution methods"; Proc. 2008 International Conference on Convergence and Hybrid Information Technology (ICHIT '08), Daejeon (Korea), 2008 August 28-30; 355-358.
13. Paul Deitel and Harvey Deitel, "Visual C# 2012 How to Program, Fifth Edition" Deitel, 2012.